SANbox2-8c/16 Switch Management

User's Guide

Information furnished in this manual is believed to be accurate and reliable. However, QLogic Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic Corporation reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic Corporation makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic Corporation assumes no responsibility for any errors that may appear in this document.

QLogic, SANbox, SANbox2, SANsurfer, and SANblade are trademarks or registered trademarks of QLogic Corporation.

Gnome is a trademark of the GNOME Foundation Corporation.

Java and Solaris are registered trademarks of Sun Microsystems, Inc.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows NT, and Windows 2000, and Internet Explorer are trademarks of Microsoft Corporation.

Netscape Navigator and Mozilla are trademarks or registered trademarks of Netscape Communications Corporation.

Red Hat is a registered trademark of Red Hat Software Inc.

All other brand and product names are trademarks or registered trademarks of their respective owners.

Document Revision History
Release, Revision A, November 2003
Release, Revision B, January 2004

© 2000–2004 QLogic Corporation
First Printed: May 2001
All Rights Reserved Worldwide.
Printed in U.S.A.

Table of Contents

Section 1 Introduction

1.1 Intended Audience 1-1
1.2 Related Materials 1-1
1.3 JDOM License 1-2
1.4 Technical Support 1-3
1.4.1 Availability 1-3
1.4.2 Training 1-3
1.4.3 Contact Information 1-3

Section 2 Using SANbox Manager

2.1 Installing SANbox Manager 2-1
2.1.1 SANsurfer Management Suite Disk - Windows Installation 2-2
2.1.2 SANsurfer Management Suite Disk - Linux Installation 2-3
2.1.3 SANsurfer Management Suite Disk - Solaris Installation 2-4
2.2 Starting SANsurfer Management Suite 2-5
2.3 Exiting SANsurfer Management Suite 2-6
2.4 Uninstalling SANsurfer Management Suite 2-8
2.4.1 SANbox Manager Installation Disk - Windows Installation 2-8
2.4.2 SANbox Manager Installation Disk - Linux Installation 2-9
2.4.3 SANbox Manager Installation Disk - Solaris Installation 2-9
2.5 Starting SANbox Manager 2-10
2.6 Exiting SANbox Manager 2-11
2.7 Uninstalling SANbox Manager 2-13
2.8 Changing the Encryption Key for the Default Fabric View File 2-13
2.9 Saving and Opening Fabric View Files 2-14
2.10 Setting SANbox Manager Preferences 2-14
2.11 Using Online Help 2-16
2.12 Viewing Software Version and Copyright Information 2-16
2.13 SANbox Manager User Interface 2-17
2.13.1 Menu Bar 2-18
2.13.1.1 Topology Display Menu Bar 2-18
2.13.1.2 Faceplate Display Menu Bar 2-19
2.13.1.3 Topology Display Shortcut Keys 2-20
2.13.1.4 Faceplate Display Shortcut Keys 2-21
2.13.2 Tool Bar 2-22
2.13.3 Fabric Tree 2-23

2.13.4 Graphic Window ... 2-24
2.13.5 Data Window and Tabs ... 2-24
2.13.6 Working Status Indicator ... 2-24
2.14 Using the Topology Display ... 2-25
2.14.1 Switch and Link Status ... 2-25
2.14.2 Working with Switches and Links ... 2-26
2.14.2.1 Selecting Switches and Links ... 2-26
2.14.2.2 Arranging Switches in the Display ... 2-26
2.14.3 Opening the Faceplate Display and Topology Popup Menus ... 2-26
2.14.4 Topology Data Windows ... 2-27
2.15 Using the Faceplate Display ... 2-28
2.15.1 Port Views and Status ... 2-28
2.15.2 Working with Ports ... 2-29
2.15.2.1 Selecting Ports ... 2-29
2.15.2.2 Opening the Faceplate Popup Menu ... 2-29
2.15.3 Faceplate Data Windows ... 2-30

Section 3 Managing Fabrics

3.1 Fabric Security ... 3-1
3.1.1 User Account Security ... 3-1
3.1.2 Fabric Services ... 3-2
3.1.2.1 Enabling SNMP Configuration ... 3-2
3.1.2.2 Enabling In-band Management ... 3-3
3.2 Managing the Fabric Database ... 3-3
3.2.1 Adding a Fabric ... 3-3
3.2.2 Removing a Fabric ... 3-4
3.2.3 Opening a Fabric View File ... 3-4
3.2.4 Saving a Fabric View File ... 3-4
3.2.5 Rediscovering a Fabric ... 3-5
3.2.6 Adding a New Switch to a Fabric ... 3-5
3.2.7 Replacing a Failed Switch ... 3-6
3.2.8 Deleting Switches and Links ... 3-7
3.3 Displaying Fabric Information ... 3-7
3.3.1 Fabric Status ... 3-7
3.3.2 Displaying the Event Browser ... 3-9
3.3.2.1 Filtering the Event Browser ... 3-11
3.3.2.2 Sorting the Event Browser ... 3-12
3.3.2.3 Saving the Event Browser to a File ... 3-12
3.3.3 Active Zone Set Data Window ... 3-12
3.4 Zoning a Fabric ... 3-13

3.4.1 Zoning Concepts ... 3-13
3.4.1.1 Zones ... 3-14
3.4.1.2 Aliases ... 3-15
3.4.1.3 Zone Sets ... 3-15
3.4.1.4 Zoning Database ... 3-16
3.4.1.5 Zoning Configuration ... 3-16
3.4.2 Using the Zoning Config Dialog ... 3-17
3.4.2.1 FC-SW-2 Auto Save ... 3-17
3.4.2.2 Default Visibility ... 3-17
3.4.3 Restoring Default Zoning ... 3-18
3.4.4 Merging Fabrics and Zoning ... 3-18
3.4.4.1 Zone Merge Failure ... 3-18
3.4.4.2 Zone Merge Failure Recovery ... 3-18
3.4.5 Using the Edit Zoning Dialog ... 3-19
3.4.6 Managing Zone Sets ... 3-22
3.4.6.1 Creating a Zone Set ... 3-22
3.4.6.2 Activating and Deactivating a Zone Set ... 3-23
3.4.6.3 Copying a Zone to a Zone Set ... 3-23
3.4.6.4 Removing a Zone from a Zone Set or from All Zone Sets ... 3-23
3.4.6.5 Removing a Zone Set ... 3-24
3.4.6.6 Removing All Zoning Definitions ... 3-24
3.4.7 Managing Zones ... 3-24
3.4.7.1 Creating a Zone in a Zone Set ... 3-25
3.4.7.2 Adding Zone Members ... 3-26
3.4.7.3 Creating a Member ... 3-26
3.4.7.4 Renaming a Zone or a Zone Set ... 3-27
3.4.7.5 Removing a Zone Member ... 3-27
3.4.7.6 Removing a Zone from a Zone Set ... 3-27
3.4.7.7 Removing a Zone from All Zone Sets ... 3-27
3.4.7.8 Changing Zone Types ... 3-28
3.4.8 Managing Aliases ... 3-28
3.4.8.1 Creating an Alias ... 3-28
3.4.8.2 Adding a Member to an Alias ... 3-29
3.4.8.3 Removing an Alias from All Zones ... 3-29
3.4.9 Saving the Zoning Database to a File ... 3-30

Section 4 Managing Switches

4.1 Managing User Accounts ... 4-1
4.1.1 Creating User Accounts ... 4-3
4.1.2 Removing a User Account ... 4-4

4.1.3 Changing a User Account Password 4-5
4.1.4 Modifying a User Account 4-6
4.2 Displaying Switch Information 4-7
4.2.1 Name Server Data Window 4-8
4.2.2 FDMI Data Window 4-9
4.2.3 Switch Data Window 4-10
4.2.4 Link Data Window 4-13
4.2.5 Port Statistics Data Window 4-13
4.2.6 Port Information Data Window 4-13
4.2.7 Configured and Active Zonesets Data Windows 4-14
4.3 Configuring Port Threshold Alarms 4-15
4.4 Exporting Name Server Information to a File 4-17
4.5 Exporting FDMI Information to a File 4-17
4.6 Paging a Switch 4-17
4.7 Setting the Date and Time 4-17
4.8 Setting Temperature Thresholds 4-18
4.9 Resetting a Switch 4-19
4.10 Configuring a Switch 4-20
4.10.1 Using the Configuration Wizard 4-21
4.10.2 Switch Properties 4-21
4.10.2.1 Symbolic Name 4-22
4.10.2.2 Switch Administrative States 4-22
4.10.2.3 Domain ID and Domain ID Lock 4-23
4.10.2.4 Fabric Device Management Interface 4-23
4.10.2.5 Broadcast Support 4-24
4.10.2.6 In-band Management 4-24
4.10.2.7 FC-SW-2 Compliance for Zoning 4-25
4.10.2.8 Legacy Port Address Format 4-25
4.10.2.9 Timeout Values 4-25
4.10.3 Network Properties 4-26
4.10.3.1 IP Configuration 4-27
4.10.3.2 SNMP Configuration 4-28
4.10.3.3 SNMP Trap Configuration 4-29
4.10.3.4 Remote Logging 4-29
4.11 Archiving a Switch 4-30
4.12 Restoring a Switch 4-30
4.13 Restoring the Factory Default Configuration 4-32
4.14 Managing Firmware 4-34
4.14.1 Installing Firmware 4-34

4.14.2 Activating the Pending Firmware 4-35
4.14.3 Changing the Pending Firmware 4-35
4.14.4 Displaying Hardware Status 4-36

Section 5 Managing Ports

5.1 Displaying Port Information 5-1
5.1.1 Monitoring Port Status 5-2
5.1.1.1 Displaying Port Types 5-2
5.1.1.2 Displaying Port Operational States 5-3
5.1.1.3 Displaying Port Speeds 5-3
5.1.1.4 Displaying Transceiver Media Status 5-4
5.1.2 Port Statistics Data Window 5-4
5.1.3 Port Information Data Window 5-7
5.1.4 Name Server Data Window 5-9
5.2 Configuring Ports 5-10
5.2.1 Changing Port Administrative States 5-11
5.2.2 Changing Port Speeds 5-12
5.2.3 Changing Port Types 5-12
5.2.4 Changing Interoperability Credits 5-13
5.2.5 Changing Port Symbolic Name 5-14
5.2.6 I/O Stream Guard 5-14
5.2.7 Scan Device 5-14
5.2.8 Extending Port Credits 5-14
5.3 Resetting a Port 5-16
5.4 Testing Ports 5-16

Appendix A Command Line Interface

A.1 Logging On to a Switch A-1
A.2 User Accounts A-1
A.3 Working with Switch Configurations A-2
A.3.1 Modifying a Configuration A-2
A.3.2 Backing up and Restoring Switch Configurations A-3
A.4 Commands A-5
Admin Command A-7
Alias Command A-8
Config Command A-10
Date Command A-13
Fallback Command A-14
Hardreset Command A-15
Help Command A-16

History Command A-17
Hotreset Command A-18
Image Command A-19
Lip Command A-20
Passwd Command A-21
Ping Command A-22
Ps Command A-23
Quit Command A-24
Reset Command A-25
Set Command A-30
Set Config Command A-32
Set Log Command A-43
Set Port Command A-46
Set Setup Command A-48
Show Command A-53
Show Config Command A-65
Show Log Command A-68
Show Perf Command A-71
Show Setup Command A-73
Shutdown Command A-75
Test Command A-76
Uptime Command A-79
User Command A-80
Whoami Command A-83
Zone Command A-84
Zoneset Command A-88
Zoning Command A-90

Appendix B Graphing Port Performance

B.1 Starting SANsurfer Fabric View B-2
B.2 Exiting SANsurfer Fabric View B-2
B.3 Saving and Opening Fabric View Files B-4
B.4 Changing the Default Fabric View File Encryption Key B-4
B.5 Setting SANsurfer Fabric View Preferences B-4
B.6 Setting the Polling Frequency B-5
B.7 Displaying Graphs B-5
B.7.1 Arranging Graphs in the Display B-6
B.7.2 Customizing Graphs B-6
B.8 Printing Graphs B-8
B.9 Rescaling a Selected Graph B-9

B.10 Saving Graph Statistics to a File B-9

Appendix C Messages

C.1 Fabrics File—Open, Save C-1
C.2 Add a Fabric C-2
C.3 Network Properties Dialog C-3
C.4 Switch Properties Dialog C-4
C.5 Port Properties Dialog C-8
C.6 Faceplate Display C-10
C.7 Firmware Fallback Dialog C-13
C.8 Load Firmware Dialog C-13
C.9 Port Loopback Test Dialog C-15
C.10 Extended Credits Wizard C-17
C.11 Zoning Dialog C-17
C.12 Restore Configuration Dialog C-20
C.13 Save Fabric View C-20
C.14 Trap Configuration Dialog C-21

Glossary

Index

Figures

Figure **Page**

2-1 Initial Startup Dialog 2-5
2-2 SANsurfer Window 2-6
2-3 Save Default Fabric View File Dialog – SANsurfer 2-7
2-4 Load Default Fabric File Dialog – SANsurfer 2-7
2-5 Initial Startup Dialog 2-10
2-6 SANbox Manager Window 2-11
2-7 Save Default Fabric View File Dialog – SANbox Manager 2-12
2-8 Load Default Fabric File Dialog – SANbox Manager 2-12
2-9 Preferences Dialog – SANbox Manager 2-15
2-10 SANbox Manager Display Elements 2-17
2-11 Topology Display Menu 2-18
2-12 Faceplate Display Menu 2-19
2-13 Fabric Tree 2-23
2-14 Topology Display 2-25
2-15 Faceplate Display 2-28
3-1 Add a New Fabric Dialog 3-3
3-2 Events Browser 3-9
3-3 Filter Events Dialog 3-11
3-4 Active Zone Set Data Window 3-13

3-5 Zoning Config Dialog ... 3-17
3-6 Edit Zoning Dialog ... 3-20
4-1 User Account Administration Dialog – Add Account ... 4-3
4-2 User Account Administration Dialog – Remove Account ... 4-4
4-3 User Account Administration Dialog– Change Password ... 4-5
4-4 User Account Administration Dialog – Modify Account ... 4-6
4-5 Faceplate Display ... 4-7
4-6 Detailed FDMI Display Dialog ... 4-10
4-7 Configured Zonesets Data Window ... 4-14
4-8 Port Threshold Alarm Configuration Dialog ... 4-15
4-9 Port Threshold Alarm Example ... 4-16
4-10 Temperature Thresholds Dialog ... 4-18
4-11 Switch Properties Dialog ... 4-22
4-12 Network Properties Dialog ... 4-26
4-13 Restore Dialogs – Full and Selective ... 4-31
4-14 Hardware Status LEDs ... 4-36
5-1 Faceplate Display – Port Information ... 5-1
5-2 Port Properties Dialog ... 5-10
5-3 Designate Donor Ports ... 5-15
5-4 Port Loopback Test Dialog ... 5-16
B-1 Fabric View Graphs ... B-1
B-2 Save Default Fabric View File Dialog – SANsurfer Fabric View ... B-3
B-3 Load Default Fabric File Dialog – SANsurfer Fabric View ... B-3
B-4 Preferences – SANsurfer Fabric View ... B-5
B-5 Default Graph Options Dialog ... B-7

Tables

Table **Page**

2-1 Management Workstation Requirements ... 2-1
2-2 Topology Display Menu Shortcut Keys ... 2-20
2-3 Faceplate Display Menu Shortcut Keys ... 2-21
2-4 Tool Bar Buttons ... 2-22
3-1 Topology Display Switch and Status Icons ... 3-8
3-2 Severity Levels ... 3-10
3-3 Edit Zoning Dialog Tool Bar Buttons and Icons ... 3-21
4-1 Factory User Accounts ... 4-2
4-2 Name Server Data Window Entries ... 4-8
4-3 FDMI Data Window Entries ... 4-9
4-4 Switch Data Window Entries ... 4-10
4-5 Switch Resets ... 4-20
4-6 Switch Administrative States ... 4-23
4-7 Timeout Values ... 4-26
4-8 IP Configuration Parameters ... 4-27
4-9 SNMP Configuration Parameters ... 4-28
4-10 SNMP Trap Configuration Parameters ... 4-29

4-11 Factory Default Configuration Settings 4-32
5-1 Port Types 5-2
5-2 Port Operational States 5-3
5-3 Port Speeds 5-3
5-4 Transceiver Media View 5-4
5-5 Port Statistics Data Window Entries 5-5
5-6 Port Information Data Window Entries 5-7
5-7 Port Administrative States 5-11
5-8 Port Speeds 5-12
5-9 Port Types 5-12
A-1 Command-Line Completion A-5
A-2 Commands Listed by Authority Level A-6
A-3 Switch Configuration Defaults A-26
A-4 Port Configuration Defaults A-27
A-5 Port Threshold Alarm Configuration Defaults A-27
A-6 Zoning Configuration Defaults A-28
A-7 SNMP Configuration Defaults A-28
A-8 System Configuration Defaults A-29
A-9 Set Config Port Parameters A-32
A-10 Set Config Switch Parameters A-35
A-11 Set Config Threshold Parameters A-37
A-12 Set Config Zoning Parameters A-38
A-13 SNMP Configuration Settings A-48
A-14 System Configuration Settings A-49
A-15 Show Port Parameters A-55
A-16 Zoning Database Limits A-91
C-1 Fabrics File – Open, Save Messages C-1
C-2 Add a Fabric Messages C-2
C-3 Network Properties Dialog Messages C-3
C-4 Switch Properties Dialog Messages C-4
C-5 Port Properties Dialog Messages C-8
C-6 Faceplate Display Messages C-10
C-7 Firmware Fallback Dialog Messages C-13
C-8 Load Firmware Dialog Messages C-13
C-9 Port Loopback Test Dialog Messages C-15
C-10 Extended Credits Wizard Messages C-17
C-11 Zoning Dialog Messages C-17
C-12 Restore Configuration Dialog Messages C-20
C-13 Save Fabric View Messages C-20
C-14 Trap Configuration Dialog Messages C-21

Notes

Section 1

Introduction

This manual describes the switch management tools which include the SANbox Manager™ application (version 4.00) and the Command Line Interface (CLI) for the SANbox2®-8c and SANbox2-16 Fibre Channel switches (firmware version 4.0). The SANbox Manager switch management application is the primary focus of this manual which is organized as follows:

- Section 1 describes the intended audience for this manual, related materials, and technical support.
- Section 2 describes how to use SANbox Manager, its menus, and its displays.
- Section 3 describes fabric management tasks.
- Section 4 describes switch management tasks.
- Section 5 describes port and device management tasks.
- Appendix A describes the command line interface.
- Appendix B describes the performance monitoring application, Fabric View.
- Appendix C describes the SANbox Manager error messages.

A glossary of terms and an index are also provided.

1.1 Intended Audience

This manual introduces the switch management products and explains their installation and use. It is intended for users responsible for installing and using switch management tools.

1.2 Related Materials

Refer to the following manuals for information about switch hardware and installation.

- *SANbox2-8c Fibre Channel Switch Installation Guide*, publication number 59042-05 Rev. B.
- *SANbox2-16 Fibre Channel Switch Installation Guide*, publication number 59021-08 Rev. B.

1.3 JDOM License

This product includes software developed by the JDOM Project (http://www.jdom.org/). Copyright (C) 2000-2002 Brett McLaughlin & Jason Hunter. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.
3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact license@jdom.org.
4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management (pm@jdom.org).

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)."

Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Brett McLaughlin <brett@jdom.org> and Jason Hunter <jhunter@jdom.org>. For more information on the JDOM Project, please see <http://www.jdom.org/>.

1.4 Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic switch products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Visit the QLogic support Web site listed in Contact Information for the latest firmware and software updates.

1.4.1 Availability

QLogic Technical Support is available from 7:00 AM to 7:00 PM Central Standard Time, Monday through Friday, excluding QLogic-observed holidays.

1.4.2 Training

QLogic offers certification training for the technical professional for both the SANblade™ HBAs and the SANbox2™ switches. From the training link at www.qlogic.com, you may choose Electronic-Based Training or schedule an intensive "hands-on" Certification course.

Technical Certification courses include installation, maintenance and troubleshooting QLogic SAN products. Upon demonstrating knowledge using live equipment, QLogic awards a certificate identifying the student as a Certified Professional. The training professionals at QLogic may be reached by email at tech.training@qlogic.com

1.4.3 Contact Information

Address:	QLogic Corporation 6321 Bury Drive Eden Prairie, Minnesota 55346-1739 USA
Telephone:	+1 952-932-4040
Fax:	+1 952-932-4018
Email: Technical Service Technical Training	 support@qlogic.com tech.training@qlogic.com
QLogic Web Site:	www.qlogic.com
Technical Support Web Site:	http://support.qlogic.com

Notes

Section 2

Using SANbox Manager

This section describes how to use the SANbox Manager application and its menus. The following topics are covered:

- Installing SANbox Manager
- Starting SANbox Manager
- Exiting SANbox Manager
- Uninstalling SANbox Manager
- Changing the encryption key for the default fabric view file
- Saving and opening fabric view files
- Setting SANbox Manager user preferences
- Using online help
- Viewing software version and copyright information
- SANbox Manager user interface
- Using the topology display
- Using the faceplate display

2.1 Installing SANbox Manager

The SANbox Manager application requires a management workstation with the characteristics described in Table 2-1.

Table 2-1. Management Workstation Requirements

Operating System	■ Windows® NT/2000/2003 ■ Linux® 7.2 Red Hat®, Gnome™ 1.4 ■ Solaris™ 2.8/2.9, CDE
Memory	256 MB or more
Disk Space	150 MB per installation
Processor	300 MHz or faster
Hardware	CD-ROM drive, RS-232 serial port, RJ-45 Ethernet port
Internet Browser	Microsoft® Internet Explorer®, Netscape Navigator®, or Mozilla™

Your switch was shipped with either a SANsurfer Management Suite Disk or a SANbox2 Installation Disk. Refer to the following installation instructions that correspond to your situation:

- SANsurfer Management Suite Disk - Windows Installation
- SANsurfer Management Suite Disk - Linux Installation
- SANsurfer Management Suite Disk - Solaris Installation
- SANbox Manager Installation Disk - Windows Installation
- SANbox Manager Installation Disk - Linux Installation
- SANbox Manager Installation Disk - Solaris Installation

2.1.1 SANsurfer Management Suite Disk - Windows Installation

To install the SANsurfer application on Windows from the SANsurfer® Management Suite Disk, do the following:

1. Close all programs currently running, and insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If the SANsurfer Management Suite start page does not open in your default browser, do the following:
   a. Using Windows Explorer, double-click the drive letter which contains the SANsurfer Management Suite Disk.
   b. Locate and double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page in your default browser.
2. On the SANsurfer Management Suite start page, click the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 (2Gb) Series area.
4. In the Operating System column, click the **Win NT/2000** link.
5. Click the **SANsurfer Management Software** link to open the File Download dialog.
6. You have a choice of running the installation file from the CD-ROM or downloading the installation file to your hard drive. Choose one of the following:
   - Open the installation file from the CD-ROM and follow the SANbox Manager installation instructions.
   - Specify a location in which to save the **sansurfer_windows_install.exe** file, and click the **Save** button. Double-click the saved **sansurfer_windows_install.exe** file and follow the SANsurfer installation instructions.

2.1.2
SANsurfer Management Suite Disk - Linux Installation

To install the SANsurfer application on Linux from the SANsurfer Management Suite Disk, do the following:

1. Insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If a file browser dialog opens showing icons for the contents of the CD-ROM, double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page. If a file browser does not open, double-click the CD-ROM icon to open the browser. If there is no CD-ROM icon, do the following:
   a. Open an xterm or other terminal window.
   b. Mount the CD-ROM. From a shell prompt, enter the following command:

      ```
      mount /mnt/cdrom
      ```

   c. Execute your web browser to view the **Start_Here.htm** document using one of the following commands:

      ```
      mozilla file:/mnt/cdrom/Start_Here.htm
      ```

      or

      ```
      netscape file:/mnt/cdrom/Start_Here.htm
      ```

   d. The SANsurfer Management Suite start page opens in your browser.
2. On the SANsurfer Management Suite start page, click the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 (2Gb) Series area.
4. In the Operating System column, click the **Linux** link.
5. Click the **SANsurfer Management Software** link to open the File Download dialog.
6. Enter a path name to save the **sansurfer_linux_install.bin** file, and click the **Save** button.
7. Open a terminal window for the directory in which the **sansurfer_linux_install.bin** file was saved, and make the file executable:

   ```
   chmod +x sansurfer_linux_install.bin
   ```

8. Execute the install program:

   ```
   ./sansurfer_linux_install.bin
   ```

9. Follow the SANsurfer installation instructions.

2.1.3
SANsurfer Management Suite Disk - Solaris Installation

To install the SANsurfer application on Solaris from the SANsurfer Management Suite CD-ROM, do the following:

1. Insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If the SANsurfer Management Suite start page does not open in your default browser, do the following:
   a. Right-click the Workspace Menu.
   b. Select **File**, then select **File Manager**.
   c. In File Manager, double-click the CD-ROM folder, and then double-click the Sansurfer folder.
   d. In the Sansurfer folder, double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page in your default browser.
2. On the SANsurfer Management Suite start page, click the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox2 (2Gb) Series area.
4. In the Operating System column, click the **Solaris SPARC** link.
5. Click the **SANsurfer Management Software** link to open the Save As dialog.
6. Enter a path name to save the **sansurfer_solaris_install.bin** file and click the **Save** button.
7. Open a terminal window for the directory in which the **sansurfer_solaris_install.bin** file was saved, and enter the following command:

   ```
   chmod +x sansurfer_solaris_install.bin
   ```

8. Execute the install program:

   ```
   ./sansurfer_solaris_install.bin
   ```

9. Follow the SANsurfer installation instructions.

Note: If you download SANsurfer from a server, be sure the downloaded file has execute permission before installing.

2.2 Starting SANsurfer Management Suite

To start the SANsurfer application for the first time, choose one of the following methods:

- For a Windows platform, double-click the SANsurfer shortcut, or select SANsurfer from Start menu, depending on how you installed the SANsurfer application. From a command line, you can enter the SANsurfer command:

  ```
  <install_directory>\SANsurfer.exe
  ```

- For a Linux platform, enter the SANbox_Manager command:

  ```
  <install_directory>/SANsurfer
  ```

- For a Solaris platform, enter the SANbox_Manager command:

  ```
  <install_directory>/SANsurfer
  ```

The application opens with the Initial Start dialog shown in Figure 2-1. If you prefer not to see this dialog, check the **Don't show this dialog again** check box. This has the same effect as disabling the Display Initial Startup Dialog preference. Refer to "Setting SANbox Manager Preferences" on page 2-14 for information about setting preferences.

Note: If a preferences file exists with the Display Initial Startup Dialog preference disabled, the Initial Start dialog will not be displayed.

Figure 2-1. Initial Startup Dialog

- Click the **Open Existing Fabric** radio button to open the Add a New Fabric dialog, which prompts you for a fabric name, IP address, account name, and password. Refer to ”Adding a Fabric” on page 3-3.
- Click the **Open Existing Fabric View File** radio button to open the Open View dialog which prompts you to specify a fabric view file that you saved earlier. Refer to ”Opening a Fabric View File” on page 3-4.
- Click the **Start Application Without Specifying a Fabric** radio button to open the SANbox Manager window shown in Figure 2-6.
- Click the **Open Configuration Wizard** radio button to open the Config Wizard to configure a switch, add a new switch, replace/restore a switch, or recover or edit an IP configuration of an existing switch.

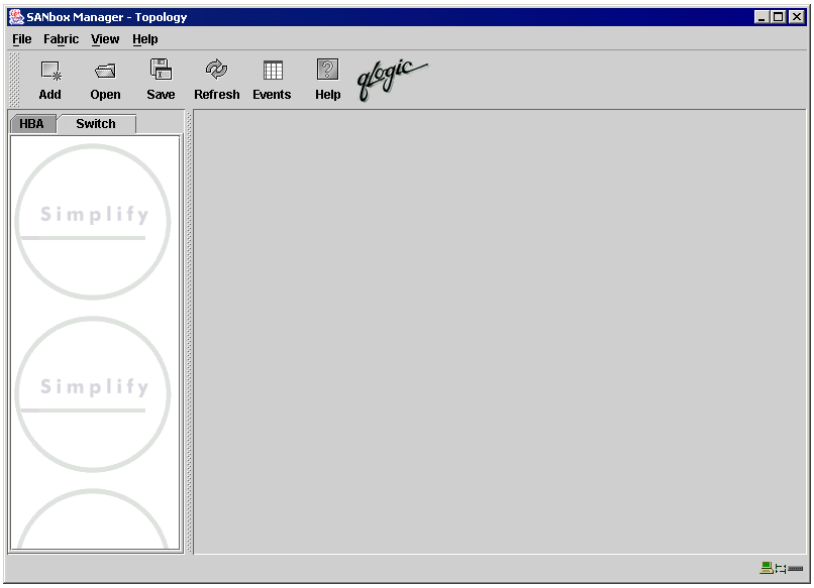


Figure 2-2. SANsurfer Window

2.3 Exiting SANsurfer Management Suite

To exit a SANsurfer application session, open the File menu and select **Exit**. If an encryption key has been defined, the current fabric view is automatically saved to your default fabric view file upon exit. The encryption key is used to encrypt the sensitive data in the default fabric view file.

If you have not yet defined an encryption key, the Save Default Fabric View File dialog, shown in Figure 2-7, prompts you to save the current fabric view as the default fabric view file. Refer to ”Changing the Encryption Key for the Default Fabric View File” on page 2-13 for information about changing this encryption key.

In the Save Default Fabric View File dialog, enter an encryption key in the Default Fabric File Encryption Key field. Re-enter the encryption key in the Re-enter Encryption Key to Confirm field. Click the **OK** button to save the current set of fabrics to the default fabric view file in the working directory.

To prevent SANbox Manager from prompting you to save the default fabric view file between SANbox Manager sessions, set the View File Auto Save and Load preferences setting to Enable (default). Refer to ”Setting SANbox Manager Preferences” on page 2-14 for more information.

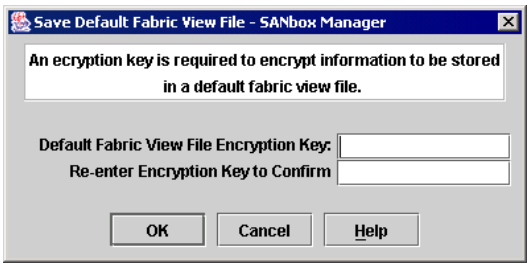

Save Default Fabric View File - SANbox Manager
An ecryption key is required to encrypt information to be stored in a default fabric view file.
Default Fabric View File Encryption Key:
Re-enter Encryption Key to Confirm
OK
Cancel
Help

Figure 2-3. Save Default Fabric View File Dialog – SANsurfer

In your next SANbox Manager session, the Load Default Fabric File dialog shown in Figure 2-4 prompts you to load the default fabric view file and to specify its encryption key, if there is one. In the Default Fabric File Encryption Key field, enter the encryption key and click the **Load View File** button. If you do not want to load the default fabric view file, click the **Continue Without Loading** button to open the SANbox Manager with no fabric displayed.

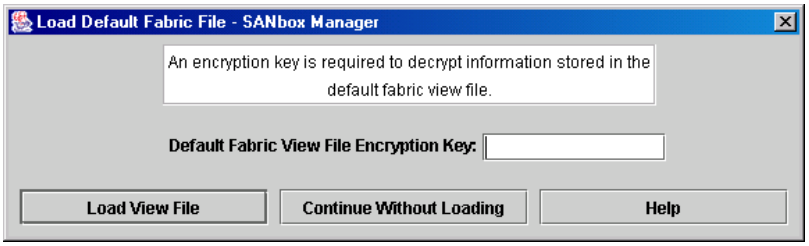

Load Default Fabric File - SANbox Manager
An encryption key is required to decrypt information stored in the default fabric view file.
Default Fabric View File Encryption Key:
Load View File
Continue Without Loading
Help

Figure 2-4. Load Default Fabric File Dialog – SANsurfer

2.4 Uninstalling SANsurfer Management Suite

A program to uninstall SANsurfer was installed as part of the SANsurfer installation process. The Uninstall Data folder in the <install_directory> contains the uninstall program (Uninstall SANsurfer).

The default installation directories are:

- For Windows: C:\Program Files\QLogic_Corporation\SANsurfer
- For Linux: /opt/QLogic_Corporation/SANsurfer
- For Solaris: /opt/QLogic_Corporation/SANsurfer

To uninstall the SANsurfer application, do the following:

- For Windows, browse for the uninstall program file or the shortcut/link that points to the uninstall program file. The uninstall program shortcut is in the same folder as the program shortcut (Start menu, program group, on desktop, or user specified) that is used to start the SANbox Manager application. Double-click the uninstall program file or shortcut/link, and follow the instructions to uninstall the SANbox Manager application.
- For Linux, execute the link to SANsurfer Uninstall.

  ```
  <install_directory>/UninstallerData/SANsurferUninstaller
  ```

- For Solaris, enter the following command and follow the instructions to uninstall the SANsurfer application:

  ```
  <install_directory>/UninstallData/SANsurferUninstaller
  ```

2.4.1 SANbox Manager Installation Disk - Windows Installation

To install the SANbox Manager application on Windows from the SANbox Manager Installation Disk, do the following:

1. Close all programs currently running, and insert the SANbox Manager Installation Disk into the management workstation CD-ROM drive.
2. Using Windows Explorer, double-click the drive letter which contains the SANbox2 Installation Disk.
3. Double click the SANbox_Manager folder, then double click the Windows folder.
4. Double click the executable file and follow the SANbox Manager installation instructions.

2.4.2
SANbox Manager Installation Disk - Linux Installation

To install the SANbox Manager application on Linux from the SANbox Manager Installation Disk, do the following:

1. Insert the SANbox2 Installation Disk into the management workstation CD-ROM drive. If a file browser does not open, double-click the CD-ROM icon to open the browser. Double click the SANbox_Manager folder, then double click the Linux folder. If there is no CD-ROM icon, do the following:
   a. Open an xterm or other terminal window.
   b. Mount the CD-ROM. From a shell prompt, enter the following command:
      ```
      mount /mnt/cdrom
      ```
   c. Change directory to location of the install program:
      ```
      cd /mnt/cdrom/SANbox_Manager/Linux
      ```
2. Execute the install program and follow the SANbox Manager installation instructions.

2.4.3
SANbox Manager Installation Disk - Solaris Installation

To install the SANbox Manager application on Solaris from the SANbox Manager Installation Disk, do the following:

1. Insert the SANbox2 Installation Disk into the management workstation CD-ROM drive.
2. Open a terminal window. If the disk isn't already mounted, enter the following command:
   ```
   volcheck
   ```
3. Move to the directory on the disk that contains the executable. Enter the following command:
   ```
   cd cdrom/cdrom0/sanbox_manager/solaris
   ```
4. Run the executable and follow the SANbox Manager installation instructions. Enter the following command:
   ```
   pkgadd -d sol_pkg
   ```

2.5 Starting SANbox Manager

To start the SANbox Manager application for the first time, choose one of the following methods:

- For a Windows platform, double-click the SANbox Manager shortcut, or select SANbox Manager from Start menu, depending on how you installed the SANbox Manager application. From a command line, you can enter the SANbox_Manager command:

  ```
  <install_directory>SANbox_Manager.exe
  ```

- For a Linux platform, enter the SANbox_Manager command:

  ```
  <install_directory>SANbox_Manager
  ```

- For a Solaris platform, enter the SANbox_Manager command:

  ```
  <install_directory>SANbox_Manager
  ```

The application opens with the Initial Start dialog shown in Figure 2-5. If you prefer not to see this dialog, check the **Don't show this dialog again** box. This has the same effect as disabling the Display Initial Startup Dialog preference. Refer to "Setting SANbox Manager Preferences" on page 2-14 for information about setting preferences.

Figure 2-5. Initial Startup Dialog

- Click the **Open Configuration Wizard** radio button to open the Config Wizard to configure a switch, add a new switch, replace/restore a switch, or recover or edit an IP configuration of an existing switch.
- Click the **Open Existing Fabric** radio button to open the Add a New Fabric dialog, which prompts you for a fabric name, IP address, account name, and password. Refer to "Adding a Fabric" on page 3-3.

- Click the **Open Existing Fabric View File** radio button to open the Open View dialog which prompts you to specify a fabric view file that you saved earlier. Refer to ”Opening a Fabric View File” on page 3-4.
- Click the **Start Application Without Specifying a Fabric** radio button to open the SANbox Manager window without displaying any fabric, as shown in Figure 2-6.

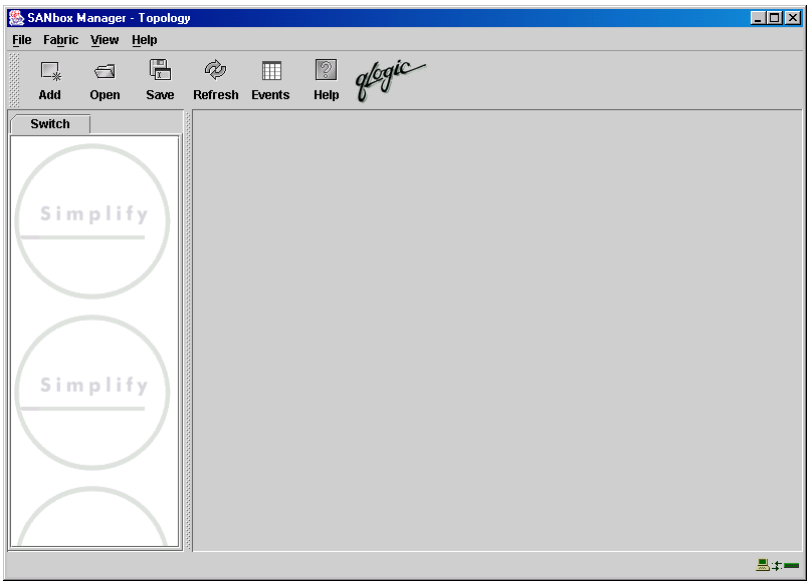


Figure 2-6. SANbox Manager Window

2.6 Exiting SANbox Manager

To exit a SANbox Manager application session, open the File menu and select **Exit**. If you have not yet defined an encryption key, the Save Default Fabric View File dialog, shown in Figure 2-7, prompts you to save the current fabric view as the default fabric view file. Enter an encryption key in the Default Fabric File Encryption Key field. Re-enter the encryption key in the Re-enter Encryption Key to Confirm field. Click the **OK** button to save the current set of fabrics to the default fabric view file in the working directory.

The encryption key is used to encrypt the sensitive data in the default fabric view file. Refer to ”Changing the Encryption Key for the Default Fabric View File” on page 2-13 for information about changing this encryption key. If an encryption key has been defined and the View File Auto Save and Load preferences setting is set to Enable, the current fabric view is automatically saved to your default fabric view file upon exit future SANbox Manager sessions.

To prevent SANbox Manager from prompting you to save the default fabric view file between SANbox Manager sessions, set the View File Auto Save and Load preferences setting to Enable (default). Refer to ”Setting SANbox Manager Preferences” on page 2-14 for more information.

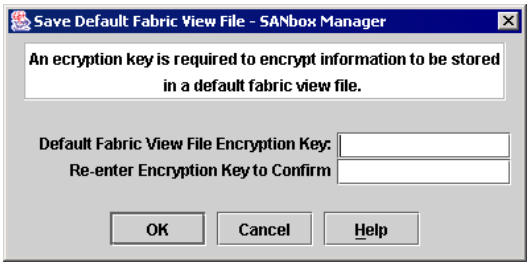

Save Default Fabric View File - SANbox Manager
An ecryption key is required to encrypt information to be stored in a default fabric view file.
Default Fabric View File Encryption Key:
Re-enter Encryption Key to Confirm
OK
Cancel
Help

Figure 2-7. Save Default Fabric View File Dialog – SANbox Manager

In your next SANbox Manager session, the Load Default Fabric File dialog shown in Figure 2-8 prompts you to load the default fabric view file and to specify its encryption key, if there is one. In the Default Fabric File Encryption Key field, enter the encryption key and click the **Load View File** button. If you do not want to load the default fabric view file, click the **Continue Without Loading** button to open the SANbox Manager with no fabric displayed.

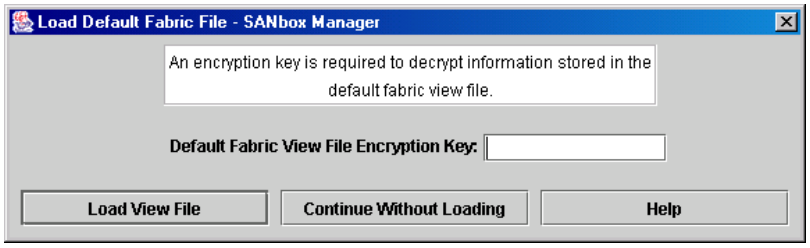

Load Default Fabric File - SANbox Manager
An encryption key is required to decrypt information stored in the default fabric view file.
Default Fabric View File Encryption Key:
Load View File
Continue Without Loading
Help

Figure 2-8. Load Default Fabric File Dialog – SANbox Manager

2.7 Uninstalling SANbox Manager

A program to uninstall SANbox Manager was installed as part of the SANbox Manager installation process. The Uninstaller Data folder in the Install folder contains the uninstall program (Uninstall SANbox Manager). Also, a shortcut/link to the uninstall program was installed in the installation directory during the SANbox Manager installation process.

The default installation directories are:

- For Windows: C:\Program Files\QLogic_Corporation\SANbox_Manager
- For Linux: /opt/QLogic_Corporation/SANbox_Manager
- For Solaris: /usr/opt/QLGCsol

To uninstall the SANbox Manager application, do the following:

- For Windows, browse for the uninstall program file or the shortcut/link that points to the uninstall program file. The uninstall program shortcut is in the same folder as the program shortcut (Start menu, program group, on desktop, or user specified) that is used to start the SANbox Manager application. Double-click the uninstall program file or shortcut/link, and follow the instructions to uninstall the SANbox Manager application.
- For Linux, execute the link to Uninstall_SANbox_Manager. If no links were created during the installation, enter the following command:

  ```
  <install_directory>UninstallerData/Uninstall_SANbox_Manager
  ```

- For Solaris, enter the following command and follow the instructions to uninstall the SANbox Manager application:

  ```
  pkgrm QLGCsol
  ```

2.8 Changing the Encryption Key for the Default Fabric View File

To change the encryption key for the SANbox Manager default fabric view file, do the following:

1. Open the File menu and select **Save Default Fabric View File** to open the Save Default Fabric View File dialog. Enter an encryption key in the Default Fabric File Encryption Key field.
2. Re-enter the same encryption key in the Re-enter Encryption Key to Confirm field.
3. Click the **OK** button to save the current set of fabrics to the default fabric view file in the working directory.

2.9 Saving and Opening Fabric View Files

A fabric view file is one or more fabrics saved to a file. In addition to the SANbox Manager default fabric view file, you can save and open your own fabric view files. To save a set of fabrics to a file, do the following:

1. Open the File menu and select **Save View As** to open the Save View dialog.
2. Enter a name for the fabric file or click the **Browse** button to select an existing file. Files are saved in the working directory.
3. Enter a password. When you attempt to open this fabric file, you will be prompted for this password. If you leave the File Password field blank, no password will be required when attempting to open this fabric file.
4. Click the **OK** button to save the view.

To open a fabric view file, do the following:

1. Open the File menu and select **Open View File** to open the Open View dialog.
2. Enter a name for the fabric file or click the **Browse** button to select an existing file.
3. If the fabric file was saved with a password, enter the password and click the **OK** button.
4. Click the **OK** button to open the view.

2.10 Setting SANbox Manager Preferences

Using the preferences settings, you can:

- Change the location of the working directory in which to save files.
- Change the location of the browser used to view the online help.
- Choose the fabric discovery interval. The fabric discovery interval is how often the SANbox Manager application receives information from the fabric. Choose 30 (default), 45, or 60 seconds. The smaller the interval, the more often the application talks to the switch and thus the greater impact to performance.
- Enable (default) or disable the view file auto save and load feature. Refer to ”Exiting SANbox Manager” on page 2-11 for more information on the default fabric view file.
- Enable (default) or disable the use of the Initial Start Dialog at the beginning of a SANbox Manager session. Refer to ”Starting SANbox Manager” on page 2-10 for information about the Initial Start Dialog. After a default fabric view file is created, this setting has no effect.

- Enable (default) or disable the Event Browser. Refer to ”Displaying the Event Browser” on page 3-9. If the Event Browser is enabled using the Preferences dialog, the next time SANbox Manager is started, all events from the switch alarm log will be displayed. If the Event Browser is disabled when SANbox Manager is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed.
- Choose the default port view when opening the faceplate display. You can set the faceplate to reflect the current port type (default), port speed, port operational state, or port transceiver media. Regardless of the default port view you choose, you can change the port view in the faceplate display by opening the View menu and selecting a different port view option. Refer to the corresponding subsection for more information:
  - ”Displaying Port Types” on page 5-2
  - ”Displaying Port Operational States” on page 5-3
  - ”Displaying Port Speeds” on page 5-3
  - ”Displaying Transceiver Media Status” on page 5-4

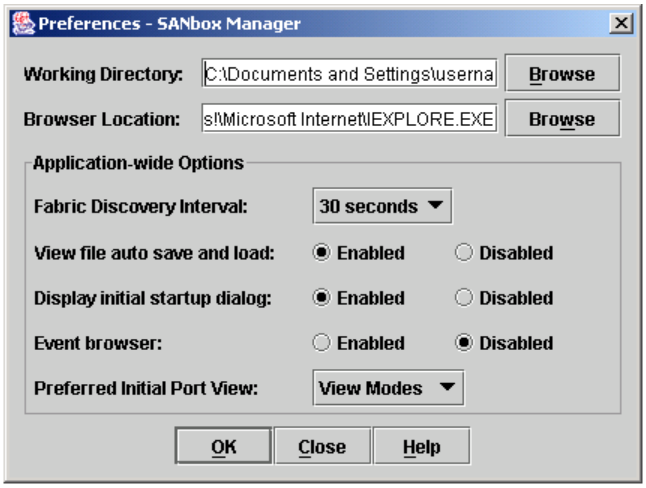


Figure 2-9. Preferences Dialog – SANbox Manager

To set preferences for your SANbox Manager sessions, do the following:

1. Open the File menu, and select **Preferences** to open the Preferences dialog.
2. Enter or browse for paths to the working directory and browser.
3. In the Application-wide Options area, choose the preferences you want.
4. Click the **OK** button to save the changes.

2.11 Using Online Help

Online help is available for the SANbox Manager application and its functions. The two ways to open the online help file are: open the Help menu and select **Help Topics**, or click the **Help** button in the tool bar. You can also display context-sensitive help for all SANbox Manager dialogs by clicking the **Help** button in the dialog.

2.12 Viewing Software Version and Copyright Information

To view SANbox Manager software version and copyright information, open the Help menu and select **About....**

2.13 SANbox Manager User Interface

The SANbox Manager application uses two basic displays to manage the fabric and individual switches: the topology display and the faceplate display. The topology display shows all switches that are able to communicate and all connections between switches. The faceplate display shows the front of a single switch and its ports. Both displays share some common elements as shown in Figure 2-10.

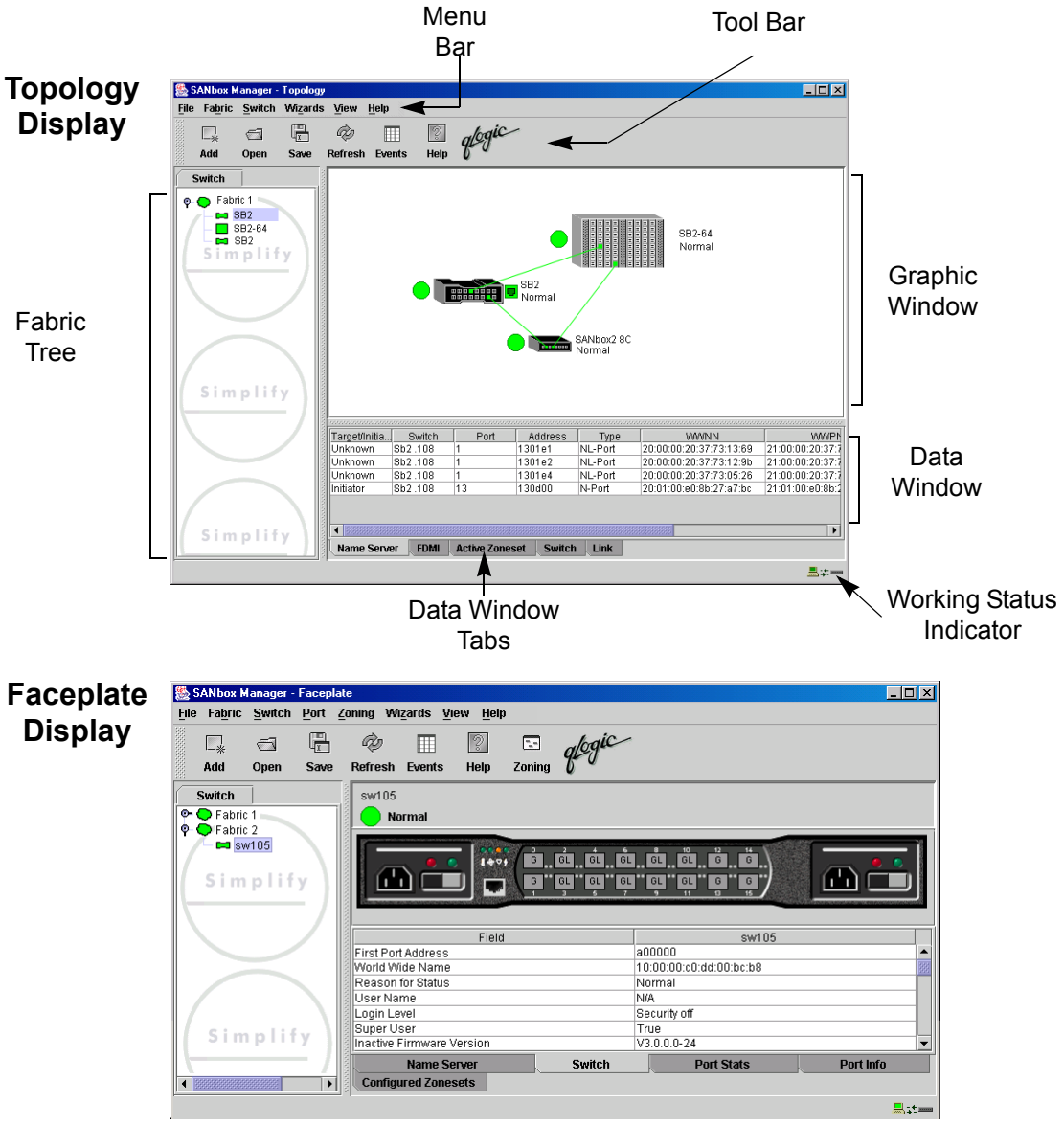


Figure 2-10. SANbox Manager Display Elements

2.13.1
Menu Bar

The SANbox Manager menus and the tasks offered in them vary depending on the display. For example, the Port menu and many of the Switch menu selections are only available in the faceplate display.

2.13.1.1
Topology Display Menu Bar

The menu options in the topology display are shown below.

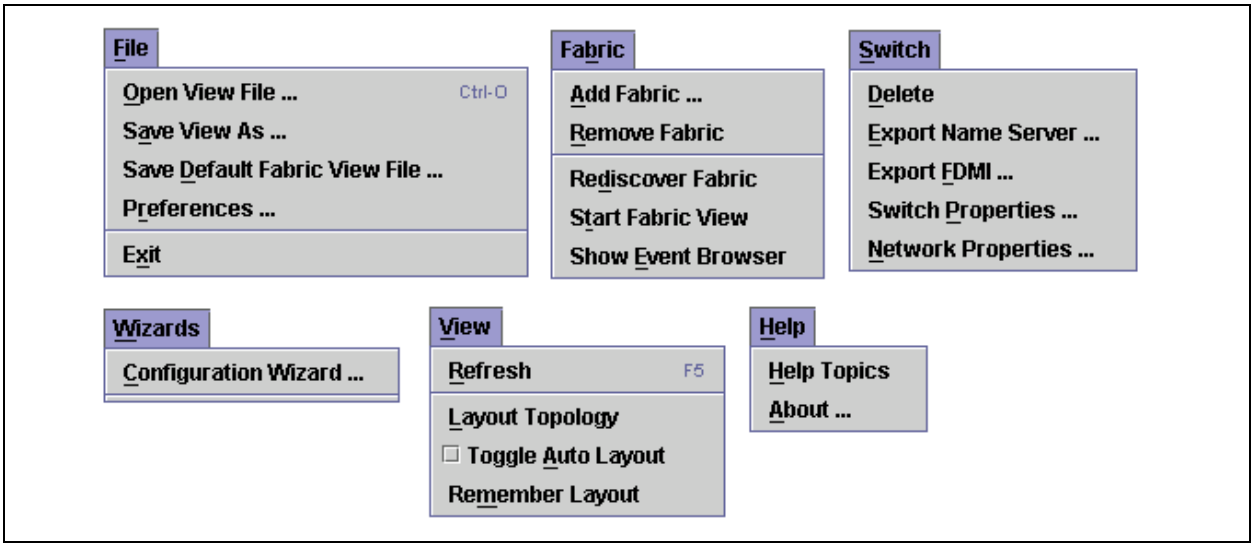


Figure 2-11. Topology Display Menu

2.13.1.2

Faceplate Display Menu Bar

The menu options in the faceplate display are shown below.

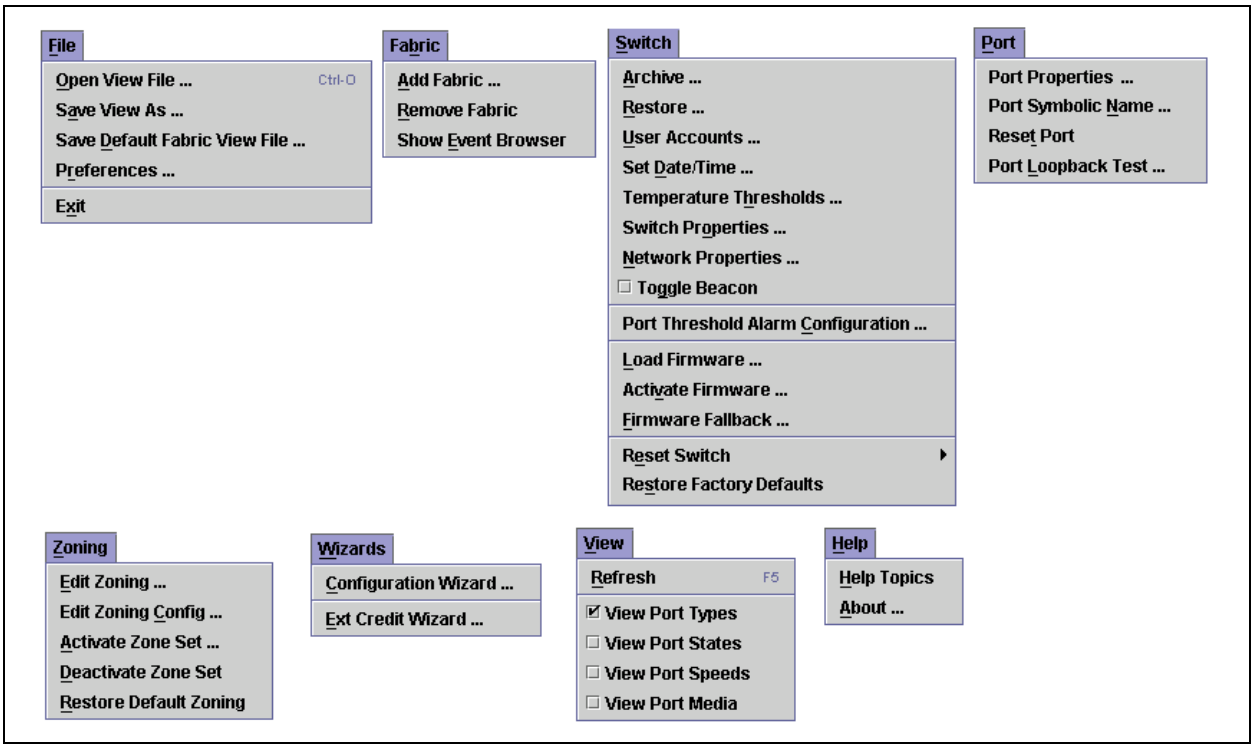


Figure 2-12. Faceplate Display Menu

The keyboard shortcut keys vary by display type: topology display and faceplate display. In addition to the menu bar, both the topology and faceplate displays have context sensitive menus that pop up when you right-click on the switches and links in the topology display, and on the switch image in the faceplate display. Refer to ”Opening the Faceplate Display and Topology Popup Menus” on page 2-26 for more information about these popup menus.

2.13.1.3

Topology Display Shortcut Keys

The shortcut keys for the topology display are below. The shortcut key combinations are not case-sensitive.

Table 2-2. Topology Display Menu Shortcut Keys

Shortcut	Selection		Shortcut	Selection
Ctrl+O Alt+F, O	File>Open View File		Alt+S, E	Switch>Export Name Server
Alt+F, A	File>Save View As		Alt+S, P	Switch>Switch Properties (active only when one switch is selected)
Alt+F, D	File>Save Default Fabric View File		Alt+S, N	Switch>Network Properties (active only when one switch is selected)
Alt+F, R	File>Preferences		Alt+W, C	Wizards> Configuration Wizard
Alt+F, X	File>Exit		Alt+V, R F5	View>Refresh
Alt+B, A	Fabric>Add Fabric		Alt+V, L	View>Layout Topology
Alt+B, R	Fabric>Remove Fabric		Alt+V, A	View>Toggle Auto Layout
Alt+B, D	Fabric>Rediscover Fabric		Alt+V, M	View>Remember Layout
Alt+B, T	Fabric>Start Fabric View		Alt+H, H	Help>Help Topics
Alt+B, E	Fabric>Show Event Browser		Alt+H, A	Help>About
Alt+S, D	Switch>Delete			

2.13.1.4

Faceplate Display Shortcut Keys

The shortcut keys for the SANbox2-8c/16 faceplate displays are shown in Table 2-3. The shortcut key combinations are not case-sensitive.

Table 2-3. Faceplate Display Menu Shortcut Keys

Shortcut	Selection		Shortcut	Selection
Ctrl+O Alt+F, O	File>Open View File		Alt+S, V	Switch>Activate Firmware
Alt+F, A	File>Save View As		Alt+S, F	Switch>Firmware Fallback
Alt+F, D	File>Save Default Fabric View File		Alt+S, E +R +h +A	Switch>Reset Switch Reset Hot Reset Hard Reset
Alt+F, R	File>Preferences		Alt+S, S	Switch>Restore Factory Defaults
Alt+F, X	File>Exit		Alt+P, R	Port>Port Properties
Alt+B, A	Fabric>Add Fabric		Alt+P, N	Port>Port Symbolic Name
Alt+B, R	Fabric>Remove Fabric		Alt+P, T	Port>Reset Port
Alt+B, E	Fabric>Show Event Browser		Alt+P, L	Port>Port Loopback Test
Alt+S, A	Switch>Archive		Alt+Z, E	Zoning>Edit Zoning
Alt+S, R	Switch>Restore		Alt+Z, C	Zoning>Edit Zoning Config
Alt+S, U	Switch>User Accounts		Alt+Z, A	Zoning>Activate Zone Set
Alt+S, D	Switch>Set Date/Time		Alt+Z, D	Zoning>Deactivate Zone Set
Alt+S, H	Switch>Temperature Thresholds		Alt+Z, R	Zoning>Restore Default Zoning
Alt+S, O	Switch>Switch Properties		Alt+W, C	Wizards> Configuration Wizard
Alt+S, N	Switch>Network Properties		Alt+W, E	Wizards> Ext Credit Wizard
Alt+S, G	Switch>Toggle Beacon		Alt+V, R F5	View>Refresh
Alt+S, C	Switch>Port Threshold Alarm Configuration		Alt+H, H	Help>Help Topics
Alt+S, L	Switch>Load Firmware		Alt+H, A	Help>About

2.13.2
Tool Bar

The tool bar consists of a row of graphical buttons that you can use to access SANbox Manager functions as shown in Table 2-4. The tool bar buttons are an alternative method to using the menu bar. The tool bar can be relocated in the display by clicking and dragging the handle at the left edge of the tool bar.

Table 2-4. Tool Bar Buttons

Tool Bar Button	Description
	Add Fabric button - adds a new fabric to the fabric view.
	Open View File button - opens an existing fabric view file.
	Save View As button - saves the current fabric view to a file.
	Refresh button - updates the topology or faceplate display with current information.
	Event Browser button - opens the events browser.
	Help Topics button - opens the online help file.
	Edit Zoning button - opens the Edit Zoning dialog (available only in faceplate display).
	The QLogic logo opens a link to the QLogic web site.

2.13.3
Fabric Tree

The fabric tree lists the managed fabrics and their switches as shown in Figure 2-13. The window width can be adjusted by clicking and dragging the moveable window border. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded or collapsed. Click this handle or double-click the entry to expand or collapse a fabric tree entry. A fabric entry expands to show its member switches.

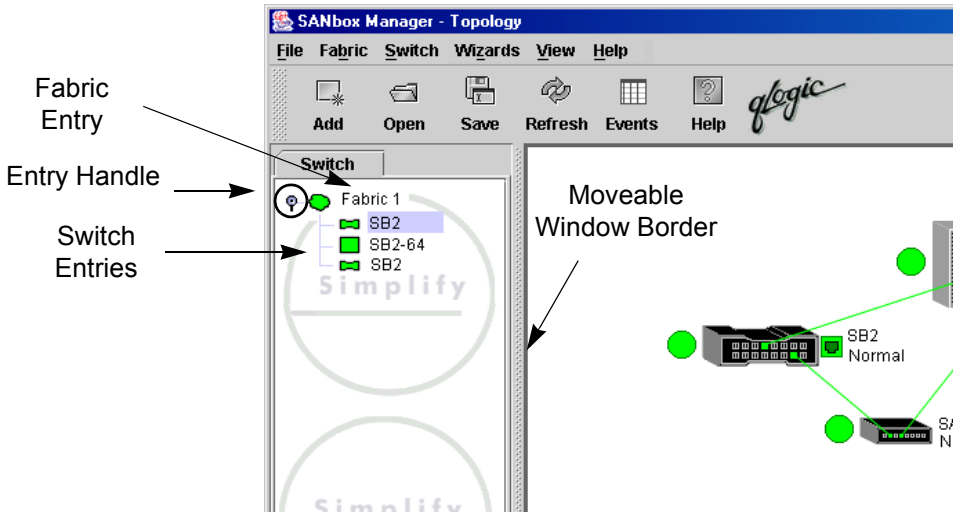


Figure 2-13. Fabric Tree

Each fabric tree entry has a small icon next to it that uses color to indicate operational status.

- A green icon indicates normal operation.
- A yellow icon indicates that a switch is operational, but may require attention to maintain maximum performance.
- A red icon indicates a potential failure, non-operational state (if switch is offline), or a switch with user authentication enabled when the fabric management switch has user authentication disabled.
- A blue icon indicates that a switch is unknown, unreachable, or unmanageable.

If the status of the fabric is not normal, the fabric icon in the fabric tree will indicate the reason for the abnormal status. The same message is provided when you rest the mouse over the fabric icon in the fabric tree.

The fabric tree provides access to the topology and faceplate displays for any fabric or switch.

- To open the topology display from the fabric tree, click a fabric entry.
- To open the faceplate display from the fabric tree, click a switch entry.

2.13.4 Graphic Window

The graphic window, as shown in Figure 2-10, presents graphic information about fabrics and switches such as the fabric topology and the switch faceplate. The window height can be adjusted by clicking and dragging the window border that it shares with the data window. This only works when displaying a fabric.

2.13.5 Data Window and Tabs

The data window presents a table of data and statistics associated with the selected tab. Use the scroll bar to browse through the data. The window length can be adjusted by clicking and dragging the border that it shares with the graphic window.

Adjust the column width by moving the pointer over the column heading border shared by two columns until a right/left arrow graphic is displayed. Click and drag the arrow to the desired width.

The data window tabs present options for the type of information to display in the data window. These options vary depending on the display.

2.13.6 Working Status Indicator

The working status indicator, located in the lower right corner of the SANbox Manager window, shows when the management workstation is exchanging information with the fabric. As conditions change, the fabric forwards this information to the management workstation where it is reflected in the various displays.

2.14 Using the Topology Display

The topology display shown in Figure 2-14 receives information from the selected fabric and displays its topology. Switches and inter-switch links (ISLs) appear in the graphic window and use color to indicate status. Consider the following topology display features:

- Switch and link status
- Working with switches and links
- Topology data windows

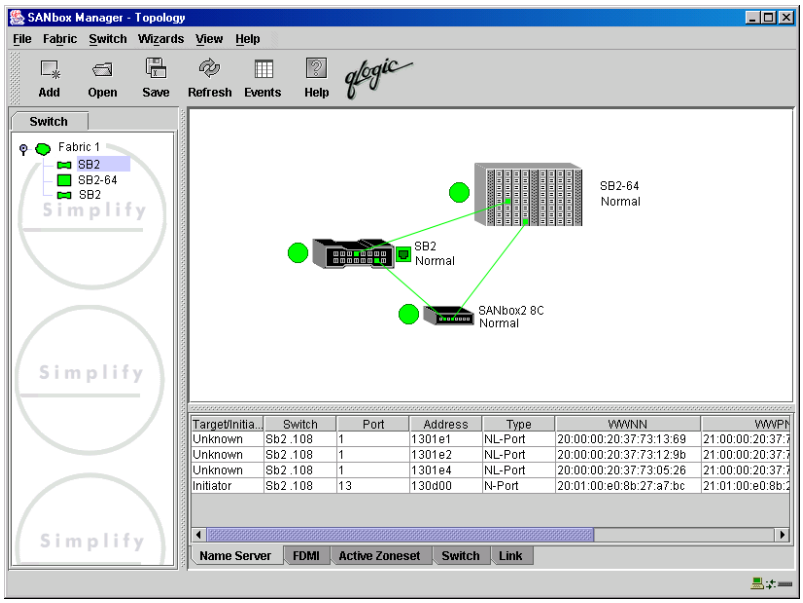


Figure 2-14. Topology Display

2.14.1 Switch and Link Status

Switch icon shape and color provide information about the switch and its operational state. Lines represent links between switches. The topology display uses green to indicate normal operation, yellow to indicate operational with errors, red to indicate a potential failure or non-operational state, and blue to indicate unknown, unreachable, or unmanageable. Refer to ”Fabric Status” on page 3-7 for more information about topology display icons.

2.14.2
Working with Switches and Links

Switch and link icons are selectable and moveable, and serve as access points for other displays and menus. You select switches and links to display information about them, modify their configuration, or delete them from the display. Context-sensitive popup menus are displayed when you right-click on a switch or link icon, or in the background of the topology display and graphic window.

2.14.2.1
Selecting Switches and Links

Selected switch icons are highlighted in light blue. Selected ISLs are displayed as a heavier line. You can select switches and links in the following ways:

- To select a switch or a link, click the icon or link.
- To select multiple switches or links, hold down the Control key and select.
- To select all switches or links, right-click anywhere in the graphic window background. Select **Select All Switches** or **Select All Links** from the popup menu.

To cancel a selection, press and hold the Control key, and select the item again. To cancel all selections, click in the graphic window background.

2.14.2.2
Arranging Switches in the Display

You can arrange individual switch icons in the topology display or allow SANbox Manager to arrange all switch icons for you:

- To move an individual switch icon, click and drag the icon to another location in the graphic window. Links stretch or contract to remain connected.
- To arrange all switch icons in the topology display automatically, open the View menu and select **Layout Topology**.

By default, the **Toggle Auto Layout** box in the View menu is checked which causes SANbox Manager to arrange the icons when you select **Layout Topology**.

You can save a custom arrangement, or layout, and restore that layout during a SANbox Manager session. Begin by arranging the icons, then open the View menu and select **Remember Layout**. To restore the saved layout, open the View menu, uncheck the **Toggle Auto Layout** box, and select **Layout Topology**.

2.14.3
Opening the Faceplate Display and Topology Popup Menus

The faceplate display shows the front of a single switch and its ports. To open the faceplate display when viewing the topology display, click the switch entry/icon in the fabric tree, or double-click the switch graphic.

The topology display also offers a fabric, switch, and a link popup menu:

- To open the fabric popup menu, right-click the graphic window background. The fabric popup menu presents selections to refresh the fabric, select all switches, select all links, or layout topology.
- To open the switch popup menu, right-click the switch icon in the graphic window. The switch popup menu presents selections to refresh the switch, delete the switch from the display, open the Switch Properties dialog, or open the Network Properties dialog.
- To open the link popup menu, right-click the link. The Link popup menu presents a selection to delete the link from the display.

2.14.4 Topology Data Windows

The topology display provides the following data windows corresponding to the data window tabs:

- Name Server – displays all devices logged with the name server and their addresses within the current fabric configuration. Refer to ”Name Server Data Window” on page 4-8 for more information.
- FDMI - displays device information from the fabric and allows end-devices to register certain information with the fabric. Refer to ”FDMI Data Window” on page 4-9 for more information.
- Active Zoneset – displays the active zone set for the fabric including zones and their member ports. Refer to ”Active Zone Set Data Window” on page 3-12 for more information about this data window. Refer to ”Zoning a Fabric” on page 3-13 for information about zone sets and zones.
- Switch – displays current network and switch configuration data for the selected switches. Refer to ”Switch Data Window” on page 4-10 for more information.
- Link – displays information about the inter-switch links. Refer to ”Link Data Window” on page 4-13 to for more information.

2.15 Using the Faceplate Display

The faceplate display shown in Figure 2-15 displays the switch name and operational state, and port status. Consider the following functional elements of the faceplate display:

- Port views and status
- Working with ports
- Faceplate data windows

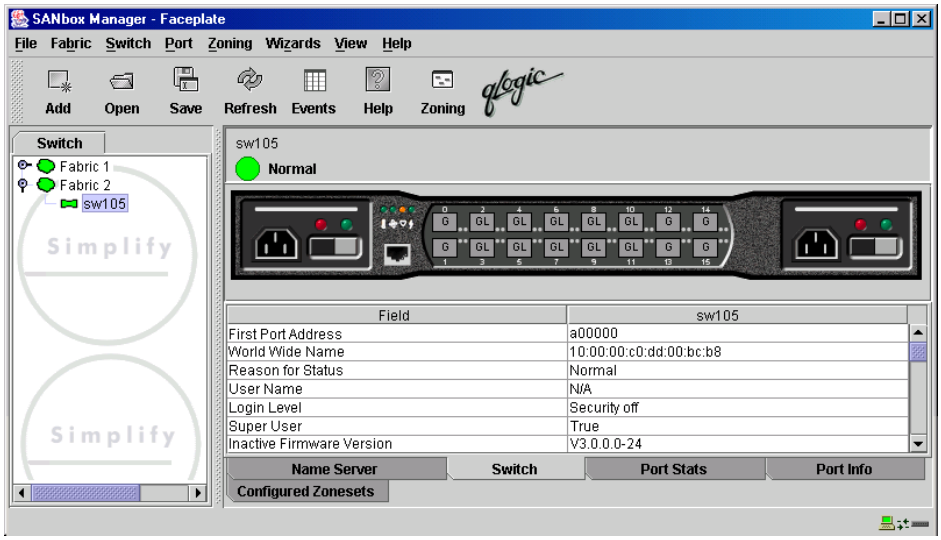


Figure 2-15. Faceplate Display

2.15.1 Port Views and Status

Port color and text provide information about the port and its operational state. Green indicates active; gray indicates inactive. The faceplate display provides the following views of port status corresponding to the View menu options in the faceplate display. Refer to ”Monitoring Port Status” on page 5-2 for more information about these displays.

- Port type
- Port state
- Port speed
- Port media

2.15.2
Working with Ports

Ports are selectable and serve as access points for other displays and menus. You select ports to display information about them in the data window or to modify them. Context-sensitive popup menus and properties dialogs are displayed when you right-click on the faceplate image or port icons in the faceplate display.

2.15.2.1
Selecting Ports

You can select ports in the following ways. Selected ports are outlined in white.

- To select a port, click the port in the faceplate display.
- To select a range of consecutive ports, select a port, then press and hold the shift key and select another port. The application selects both end ports and all ports in between in port number sequence.
- To select several non-consecutive ports, hold the Control key while selecting.
- To select all ports, right-click on the faceplate image in the graphic window. Select **Select All Ports** from the popup menu.

To cancel a selection, press and hold the Control key and select it again.

2.15.2.2
Opening the Faceplate Popup Menu

To open the popup menu, right-click on the faceplate image to present the following tasks.

- Refresh the switch
- Select all ports
- Manage switch properties
- Manage network properties
- Extended credits wizard
- Manage port properties
- Change the port symbolic name
- Run the port loopback tests

If no ports are selected, the port-related tasks will be unavailable in the menu. Right-click a port to open the Port popup menu. Hold down the Shift or Control key to select more than one port. If multiple ports are selected, right-click on one of the selected ports.

2.15.3
Faceplate Data Windows

The faceplate display provides the following data windows corresponding to the data window tabs:

- Name Server – displays all devices connected to the switch that are logged with the name server.
- Switch – displays current switch configuration data.
- Port Statistics – displays performance data for the selected ports.
- Port Information – displays information for the selected ports.
- Configured Zonesets – displays all zone sets, zones, and zone membership in the zoning database.

Section 3

Managing Fabrics

This section describes the following tasks that manage fabrics:

- Securing a fabric
- Managing the fabric database
- Displaying fabric information
- Zoning a fabric

3.1 Fabric Security

The components of Fibre Channel fabric security are:

- User account security
- Fabric services

3.1.1 User Account Security

User account security is the process by which your user account and password are authenticated with the list of valid user accounts and passwords. The switch validates your account and password when you attempt to add a fabric using SANbox Manager or log in to a switch through Telnet. Your system administrator defines accounts, passwords, and authority levels that are stored on the switch. Refer to ”Managing User Accounts” on page 4-1 for more information.

When logging in to a switch through Telnet, you must enter a user account and password to access the switch. SANbox Manager, however, does not require an user account and password to add a fabric unless the UserAuthentication parameter is enabled. The switch comes from the factory with the UserAuthentication parameter disabled. User account security is only configurable using command line interface. Use the Set Setup System command in the command line interface to enable the UserAuthentication parameter to turn on user account security. The UserAuthentication parameter must be configured the same for all switches in the fabric. Refer to the ”Set Setup Command” on page A-48 for more information.

When you add a fabric and the UserAuthentication parameter is disabled, SANbox Manager ignores the user account and password entries and logs you in using the default user account (Admin). The Admin account possesses Admin authority which grants full access to all tasks of the SANbox Manager menu system. If the UserAuthentication parameter is enabled, you must enter a user account and password. The switch validates your user account and SANbox

Manager grants access to its menus according to your authority level. If you do not have Admin authority, you are limited to monitoring tasks.

Note: If a user is logged into a switch using SANbox Manager or CLI, and an administrator changes user access rights, passwords, or UserAuthentication security settings, existing logins will not be affected by the new settings. Login access and privileges are only checked for a new login request.

3.1.2
Fabric Services

Fabric services security includes SNMP and in-band management. Simple Network Management Protocol (SNMP) is the protocol governing network management and monitoring of network devices. SNMP security consists of a read community string and a write community string, that are basically the passwords that control read and write access to the switch. The read community string ("public") and write community string ("private") are set at the factory to these well-known defaults and should be changed if SNMP is enabled using the Network Properties dialog. If SNMP is enabled (default) and the read and write community strings have not been changed from their defaults, you risk unwanted access to the switch. Refer to ”Enabling SNMP Configuration” on page 3-2 for more information. SNMP is enabled by default.

In-band management is the ability to manage switches across inter-switch links using SANbox Manager, SNMP, management server, or the application programming interface. The switch comes from the factory with in-band management enabled. If you disable in-band management on a particular switch, you can no longer communicate with that switch by means other than a direct Ethernet or serial connection. Refer to ”Enabling In-band Management” on page 3-3 for more information.

3.1.2.1
Enabling SNMP Configuration

To enable SNMP configuration, do the following:

1. On the faceplate display, open the Switch menu and select **Network Properties** to open the Network Properties dialog.
2. In the SNMP Configuration area, place a check mark in the **SNMP Enabled** check box.
3. Click the **OK** button to save the change to the database.

3.1.2.2
Enabling In-band Management

To enable In-band Management, do the following:

1. On the faceplate display, open the Switch menu and select **Switch Properties** to open the Switch Properties dialog.
2. Click the **In-band Management Enable** button.
3. Click the **OK** button to save the change to the database.

3.2
Managing the Fabric Database

A fabric database contains the set of fabrics that you have added during a SANbox Manager session. Initially, if you do not open an existing fabric or fabric view file, the SANbox Manager application opens with an empty fabric database.

3.2.1
Adding a Fabric

To add a fabric to the database, do the following:

1. Open the Fabric menu and select **Add Fabric** to open the Add a New Fabric dialog as shown in Figure 3-1.

Figure 3-1. Add a New Fabric Dialog

2. Enter a fabric name (optional) and the IP address of the switch through which to manage the fabric.
3. Enter an account name and password. The factory login name and password are (admin, password). The password is for the switch and is stored in the switch firmware. If the UserAuthentication parameter is set to False (default), you are not required to enter a login name or password. If you do enter a login name and password when UserAuthentication is set to False, these entries are ignored.

- Refer to "User Account Security" on page 3-1 for information about user authentication.
- Refer to "Managing User Accounts" on page 4-1 or the "User Command" on page A-80 for information about creating user accounts.

4. Click the **Add Fabric** button.

Note: A switch supports a combined maximum of 19 logins or sessions reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for SANbox Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins, and Telnet logins. Additional logins will be refused.

3.2.2 Removing a Fabric

To delete a fabric file from the database, do the following:

1. Select a fabric in the fabric tree.
2. Open the Fabric menu and select **Remove Fabric**.

3.2.3 Opening a Fabric View File

A fabric view file is one or more fabrics saved to a file. To open an existing view file, do the following:

1. Open the File menu and select **Open View File**, or click the **Open** button. If the fabric you are currently viewing has changed, you will be prompted to save the changes to the fabric view file with the Save View dialog before opening a different view file.
2. In the Open View dialog, enter the name of the file to open, and enter a file password, if a password was entered when this fabric view file was saved.
3. Click the **OK** button.

3.2.4 Saving a Fabric View File

To save a view file, do the following:

1. Open the File menu, and select **Save View As**.
2. In the Save View dialog, enter a new file name.

3. Enter a file password, if necessary.
4. Click the **OK** button.

3.2.5 Rediscovering a Fabric

After making changes to or deleting switches from a fabric view, it may be helpful to again view the actual fabric configuration. The rediscover fabric option clears out the current fabric information being displayed, and rediscovers all switch information. To rediscover a fabric, open the Fabric menu, and select **Rediscover Fabric**. The rediscover function is more comprehensive than the refresh function.

3.2.6 Adding a New Switch to a Fabric

If there are no special conditions to be configured for the new switch, simply plug in the switch and the switch becomes functional with the default fabric configuration. The default fabric configuration settings are:

- Fabric zoning is sent to the switch from the fabric.
- All ports will be GL_Ports.
- The default IP address 10.0.0.1 is assigned to the switch without a gateway or boot protocol configured (RARP, BOOTP, and DHCP).

If you are adding a new switch to a fabric and do not want to accept the default fabric configuration, do the following:

1. If the switch is not new, reset the switch to the factory configuration before adding the switch to the fabric by selecting **Restore Factory Defaults** in the Switch menu from the faceplate display.
2. If you want to manage the switch through the Ethernet port, you must first configure the IP address using the Network Properties dialog or the Configuration Wizard.
3. Configure any special switch settings. Consider configuring the Default Visibility setting to None in the Zoning Config dialog to prevent devices from finding other devices on all switches in the fabric until the new switch is configured. To open the Zoning Config dialog, open the Zoning menu, and select **Edit Zoning Config**.
4. Plug in the inter-switch links (ISL), but do not connect the devices.
5. Configure the port types for the new switch using the Port Properties dialog. The ports can be G_Port, GL_Port, F_Port, FL_Port, or Donor.
6. Connect the devices to the switch.
7. Make any necessary zoning changes using the Edit Zoning dialog. To open the Edit Zoning dialog, open the Zoning menu, and select **Edit Zoning**. If you changed the Default Visibility setting in the Zoning Config dialog from All

to None, change that setting back to All. To open the Zoning Config dialog, open the Zoning menu, and select **Edit Zoning Config**.

3.2.7 Replacing a Failed Switch

The archive/restore works for all switches. However, the Restore menu item is not available for the in-band switches. You can only restore a switch out-of-band (the fabric management switch). There are certain parameters that are not archived, and these are not restored by SANbox Manager. Refer to ”Archiving a Switch” on page 4-30 and ”Restoring a Switch” on page 4-30 for information about archive and restore. Use the following procedure to replace a failed switch for which an archive is available.

1. At the failed switch:
   a. Turn off the power and disconnect the AC cords.
   b. Note port locations and remove the interconnection cables and SFPs.
   c. Remove the failed switch.
2. At the replacement switch:
   a. Mount the switch in the location where the failed switch was removed.
   b. Install the SFPs using the same ports as were used on the failed switch.

      CAUTION! Do not reconnect inter-switch links, target devices, and initiator devices at this time. Doing so could invalidate the fabric zoning configuration.

   c. Attach the AC cords and power up the switch.
3. Select the failed switch in the topology display. Open the Switch menu and select **Delete**.
4. Restore the configuration from the failed switch to the replacement switch:
   a. Open a new fabric through the replacement switch.
   b. Open the faceplate display for the replacement switch. Open the Switch menu and select **Restore**.
   c. In the Restore dialog, enter the archive file from the failed switch or browse for the file.
   d. Click the **Restore** button.
5. Reset the replacement switch to activate the configuration formerly possessed by the failed switch including the domain ID and the zoning database. Open the Switch menu and select **Reset Switch**.

6. Reconnect the inter-switch links, target devices, and initiator devices to the replacement switch using the same ports as were used on the failed switch.

3.2.8 Deleting Switches and Links

The SANbox Manager application does not automatically delete switches or links that have failed or have been physically removed from the Fibre Channel network. In these cases, you can delete switches and links to bring the display up to date. If you delete a switch or a link that is still active, the SANbox Manager application will restore it automatically. You can also refresh the display. To delete a switch from the topology display, do the following:

1. Select one or more switches in the topology display.
2. Open the Switch menu and select **Delete**.

To delete a link, do the following:

1. Select one or more links in the topology display.
2. Open the Switch menu and select **Delete**.

3.3 Displaying Fabric Information

The topology display is your primary tool for monitoring a fabric. The graphic window of the topology display provides status information for switches, inter-switch links, and the Ethernet connection to the management workstation.

The data window tabs show name server, switch, and active zone set information. The Active Zoneset tab shows the zone definitions for the active zone set. Refer to ”Name Server Data Window” on page 4-8 and ”Switch Data Window” on page 4-10 for information about the Name Server and Switch data windows.

3.3.1 Fabric Status

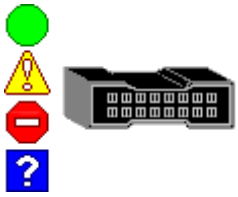
The fabric updates the topology and faceplate displays by forwarding changes in status to the management workstation as they occur. You can allow the fabric to update the display status, or you can refresh the display at any time. To refresh the topology display, do one of the following:

- Click the **Refresh** button.
- Open the View menu and select **Refresh**.
- Press the F5 key.
- Right-click anywhere in the background of the topology display and select **Refresh Fabric** from the popup menu.

The topology display uses switch and status icons to provide status information about switches, inter-switch links, and the Ethernet connection. The switch status icons, displayed on the left side of a switch, vary in shape and color. Switches

controlled by an Ethernet Internet Protocol have a colored Ethernet icon displayed on the right side of the switch. A green Ethernet icon indicates normal operation, yellow indicates a condition that may require attention to maintain maximum performance, and red indicates a potential failure. Table 3-1 shows the different switch icons and their meanings.

Table 3-1. Topology Display Switch and Status Icons

Switch Icon	Description
	SANbox2-16 Switch ■ Normal operation (Green) ■ Warning–operational with errors (Yellow) ■ Critical–potential failure (Red) ■ Unknown–communication status unknown, unreachable, or unmanageable (Blue)
	Fabric Management Switch ■ Ethernet connection normal (Green) ■ Ethernet connection warning (Yellow) ■ Ethernet connection critical (Red)
	SANbox2-8c Switch
	Switch is not manageable with this version of SANbox Manager. Use the management application that was shipped with this switch.

3.3.2
Displaying the Event Browser

The Event Browser displays a list of recorded events and alarms generated by the switches in the fabric and the SANbox Manager application. Events are generated by the SANbox Manager application and are not saved on the switch, but can be saved to a file during the SANbox Manager session. An alarm is also an event, but is generated by the switch, stored on the switch, and will be retrieved when restarting the SANbox Manager application. Entries in the Event Browser shown in Figure 3-2, are formatted by severity, time stamp, source, type, and description. The maximum number of entries allowed is 1500. Once the maximum is reached, the event list wraps and the oldest events are discarded and replaced with the new events. Alarm entries have a switch time stamp, while event entries have a workstation time stamp. You can filter, sort, and export the contents of the Event Browser to a file. The Event Browser begins recording when enabled and SANbox Manager is running.

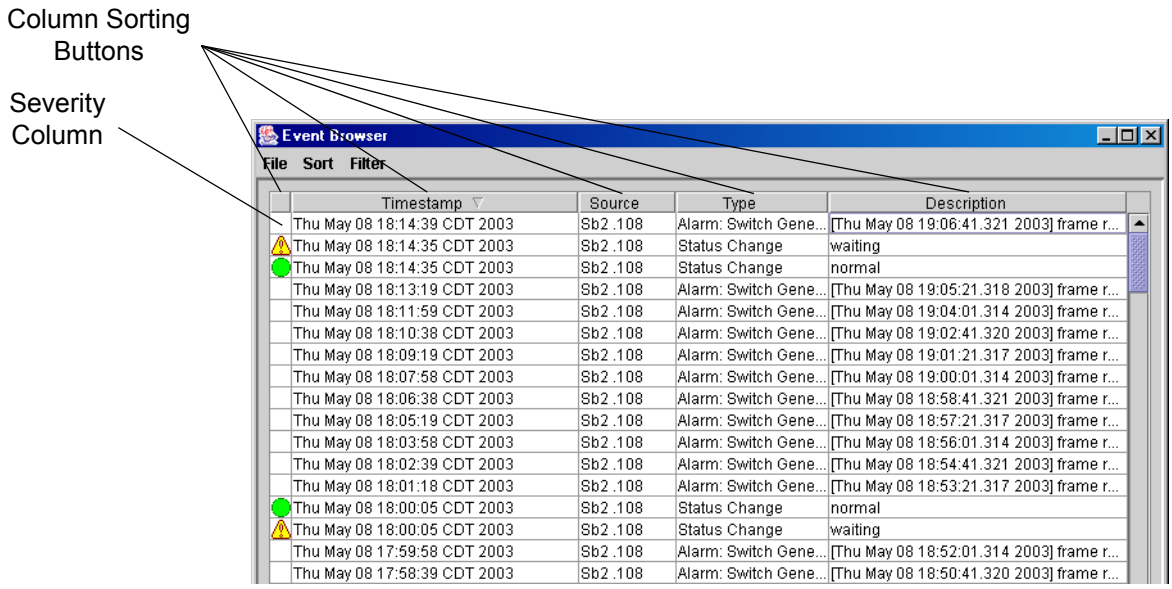

Column Sorting Buttons
Severity Column
Event Browser
File Sort Filter
Timestamp
Source
Type
Description
Thu May 08 18:14:39 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 19:06:41.321 2003] frame r...
Thu May 08 18:14:35 CDT 2003 Sb2 .108 Status Change waiting
Thu May 08 18:14:35 CDT 2003 Sb2 .108 Status Change normal
Thu May 08 18:13:19 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 19:05:21.318 2003] frame r...
Thu May 08 18:11:59 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 19:04:01.314 2003] frame r...
Thu May 08 18:10:38 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 19:02:41.320 2003] frame r...
Thu May 08 18:09:19 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 19:01:21.317 2003] frame r...
Thu May 08 18:07:58 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 19:00:01.314 2003] frame r...
Thu May 08 18:06:38 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 18:58:41.321 2003] frame r...
Thu May 08 18:05:19 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 18:57:21.317 2003] frame r...
Thu May 08 18:03:58 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 18:56:01.314 2003] frame r...
Thu May 08 18:02:39 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 18:54:41.321 2003] frame r...
Thu May 08 18:01:18 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 18:53:21.317 2003] frame r...
Thu May 08 18:00:05 CDT 2003 Sb2 .108 Status Change normal
Thu May 08 18:00:05 CDT 2003 Sb2 .108 Status Change waiting
Thu May 08 17:59:58 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 18:52:01.314 2003] frame r...
Thu May 08 17:58:39 CDT 2003 Sb2 .108 Alarm: Switch Gene... [Thu May 08 18:50:41.320 2003] frame r...

Figure 3-2. Events Browser

If the Event Browser is enabled using the Preferences dialog, the next time SANbox Manager is started all events from the switch alarm log will be displayed. If the Event Browser is disabled when SANbox Manager is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed.

To display the Event Browser, open the Fabric menu and select **Show Event Browser**, or click the **Events** button on the tool bar. If the **Show Event Browser** selection or the **Events** button is grayed-out, you must first enable the **Events**

Browser preference. Refer to ”Setting SANbox Manager Preferences” on page 2-14.

Severity is indicated in the severity column using icons as described in Table 3-2.

Note:

- The alarm log is cleared out when the switch is reset or power cycled and that the user should save these log files off if they want to keep the data. Refer to ”Set Log Command” on page A-43 for information about saving the alarm log to a file.
- Events (Critical, Warning, Normal, and Informative) are generated by the application and are not saved on the switch. They are permanently discarded when you close a SANbox Manager session, but you can save these events to a file on the workstation before you close SANbox Manager and read it later with a text editor or browser.
- Alarms are generated by the switch, stored on switch, and will be retrieved when the application is restarted. Some alarms are configurable. Refer to ”Configuring Port Threshold Alarms” on page 4-15.

Table 3-2. Severity Levels

Severity Icon	Description
	Alarm – An alarm is an event generated by the switch that specifically requests attention.
	Critical event – An event generated by the SANbox Manager application and indicates a potential failure.
	Warning event – An event generated by the SANbox Manager application that indicates errors or other conditions that may require attention to maintain maximum performance.
	Normal event – An event generated by the SANbox Manager application that indicates a transition from a non-normal to normal operation.
No icon	Informative – An unclassified event generated by the SANbox Manager application that provides supporting information.

3.3.2.1

Filtering the Event Browser

Filtering the Event Browser enables you to display only those events that are of interest based on the event severity, timestamp, source, type, and description. To filter the Event Browser, open the Filter menu and select **Filter Entries**. This opens the Filter Events dialog shown in Figure 3-3. The Event Browser displays those events that meet all of the criteria in the Filter Events dialog. If the filtering criteria is cleared or changed, then all the events that were previously hidden that satisfy the new criteria will be shown.

You can filter the event browser in the following ways:

- Severity – Check one or more of the corresponding check boxes to display alarm events, critical events, warning events, normal events, or informative events.
- Date/Time – Check one or both of the From: and To: check boxes. Enter the bounding timestamps (MM/dd/yy hh:mm:ss aa) to display only those events that fall within those times. ("aa" indicates AM or PM.) The current year (yy) can be entered as either 2 or 4 digits. For example, 12/12/03 will be interpreted December 12, 2003.
- Text – Check one or more of the corresponding check boxes and enter a text string (case sensitive) for event source, type, and description. The Event Browser displays only those events that satisfy all of the search specifications for the Source, Type, and Description text.

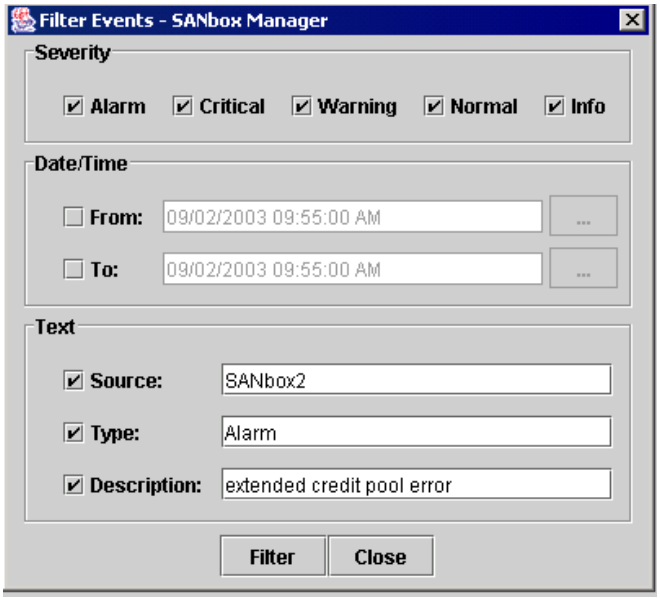


Figure 3-3. Filter Events Dialog

3.3.2.2
Sorting the Event Browser

Sorting the Event Browser enables you to display the events in alphanumeric order based on the event severity, timestamp, source, type, or description. Initially, the Event Browser is sorted in ascending order by timestamp. To sort the Event Browser, click the **Severity**, **Timestamp**, **Source**, **Type**, or **Description** column buttons. You can also open the Sort menu and select **By Severity**, **By Timestamp**, **By Source**, **By Type**, or **By Description**. Successive sort operations of the same type alternate between ascending and descending order.

3.3.2.3
Saving the Event Browser to a File

Filtering does affect the save operation; that is, only those events are saved. To save the Event Browser to a file, do the following:

1. Filter and sort the Event Browser to obtain the desired display.
2. Open the File menu and select **Save As**.
3. Select a folder and enter a file name in which to save the event log and click the **Save** button. The file is saved in XML format and can be opened with an internet browser or a text editor.

3.3.3
Active Zone Set Data Window

The Active Zoneset data window displays the zone membership for the active zone set that resides on the fabric management switch. The active zone set is the same on all switches in the fabric – you can confirm this by adding a fabric through another switch and comparing Active Zone Set displays.

To open the Active Zoneset data window, click the **Active Zoneset** tab below the data window in the topology display. Refer to ”Configured and Active Zonesets Data Windows” on page 4-14 for information about the zone set definitions on a particular switch. Refer to ”Zoning a Fabric” on page 3-13 for more information about zone sets and zones.

The Active Zoneset data window, shown in Figure 3-4, uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded. Click this handle or double-click the following entries:

- A zone set entry expands to show its member zones.
- A zone entry expands to show its member port/devices.
- WWN and FC devices that are zoned, but no longer part of the fabric, are grayed-out.

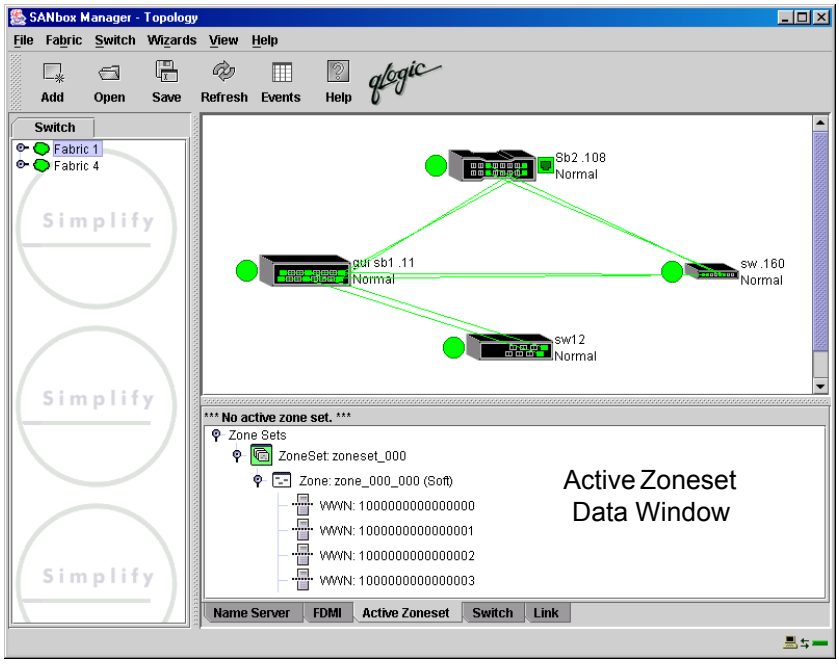


Figure 3-4. Active Zone Set Data Window

3.4
Zoning a Fabric

Zoning enables you to divide the ports and devices of the fabric into zones for more efficient and secure communication among functionally grouped nodes. This subsection addresses the following topics:

- Zoning concepts
- Using the Zoning Config dialog
- Restoring default zoning
- Using the Edit Zoning dialog
- Merging fabrics and zoning
- Managing zone sets
- Managing zones
- Managing aliases

3.4.1
Zoning Concepts

The following zoning concepts provide some context for the zoning tasks described in this section:

- Zones

- Aliases
- Zone sets
- Zoning database
- Zoning configuration

3.4.1.1
Zones

A zone is a named group of ports or devices that can communicate with each other. Devices within a zone can only communicate with other devices in the same zone. A device may participate in more than one zone.

Membership in a zone can be defined by switch domain ID and port number, device Fibre Channel address, or device World Wide Name (WWN).

- WWN entries define zone membership by the World Wide Name of the attached device. With this membership method, you can move WWN member devices to different switch ports in different zones without having to edit the member entry as you would with a domain ID/port number member. Furthermore, unlike FCID members, WWN zone members are not affected by changes in the fabric that could change the Fibre Channel address of an attached device.
- FCID entries define zone membership by the Fibre Channel address of the attached device. With this membership method you can replace a device on the same port without having to edit the member entry as you would with a WWN member.
- Domain ID/Port number entries define zone membership by switch domain ID and port number. All devices attached to the specified port become members of the zone. The specified port must be an F_Port or an FL_Port.

Two types of zones are supported. The following zone types define increasingly restrictive levels of communication.

- Soft zone
- Hard zone - Access Control List (ACL)

3.4.1.1.1
Soft Zones

Soft zoning divides the fabric for purposes of controlling discovery. Devices within the same soft zone automatically discover and communicate freely with all other members of the same zone. The soft zone boundary is not secure; traffic across soft zones can occur if addressed correctly. Soft zones that include members from multiple switches need not include the ports of the inter-switch links. Soft zone boundaries yield to ACL zone boundaries. Soft zones can overlap; that is, a device can participate in more than one soft zone. Zone membership can be

defined by Fibre Channel address, domain ID and port number, World Wide Name, or a combination. Soft zoning supports all port types.

3.4.1.1.2
Access Control List Hard Zones

Access Control List (ACL) zoning divides the fabric for purposes of controlling discovery and inbound traffic. ACL zoning is a type of hard zoning that is hardware enforced. This type of zoning is useful for controlling access to certain devices without totally isolating them from the fabric. Devices can communicate with each other and transmit outside the ACL zone, but cannot receive inbound traffic from outside the zone. The ACL zone boundary is secure against inbound traffic. ACL zones can overlap; that is, a port can be a member of more than one ACL zone. ACL zones that include members from multiple switches need not include the ports of the inter-switch links. ACL zone boundaries supersede soft zone boundaries. Membership can be defined only by domain ID and port number. ACL zoning supports all port types.

3.4.1.2
Aliases

To make it easier to add a group of ports or devices to one or more zones, you can create an alias. An alias is a named set of ports or devices that are grouped together for convenience. Unlike zones, aliases impose no communication restrictions between its members. You can add an alias to one or more zones. However, you cannot add a zone to an alias, nor can an alias be a member of another alias.

3.4.1.3
Zone Sets

A zone set is a named group of zones. A zone can be a member of more than one zone set. All zones that are not members of a zone set belong to the orphan zone set. The orphan zone set is saved on the switch. Each switch in the fabric maintains its own zoning database containing one or more zone sets. This zoning database resides in non-volatile or permanent memory and is therefore retained after a reset. Refer to ”Configured Zonesets Data Window” on page 4-14 for information about displaying the zoning database.

To apply zoning to a fabric, choose a zone set and activate it. When you activate a zone set, the switch distributes that zone set and its zones, excluding aliases, to every switch in the fabric. This zone set is known as the active zone set. Refer to ”Active Zone Set Data Window” on page 3-13 for information about displaying the active zone set.

3.4.1.4
Zoning Database

Each switch has its own zoning database. The zoning database is made up of all aliases, zones, and zone sets that have been created on the switch or received from other switches. The switch maintains two copies of the inactive zoning database: one copy is maintained in temporary memory for editing purposes; the second copy is maintained in permanent memory. Zoning database edits are made on an individual switch basis and are not propagated to other switches in the fabric when saved.

The zoning limits for a fabric are as follows:

- **MaxZoneSets is 256.** The maximum number of zone sets that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.
- **MaxZones is 256**. The maximum number of zones that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.
- **MaxAliases is 256**. The maximum number of aliases that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.
- **MaxTotalMembers is 2000**. The maximum number of total zone and alias members that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric. Aliases are considered zone members since they can be added to a zone just like a normal zone member.
- **MaxZonesInZoneSets is 1000**. The maximum number of zone linkages to zonesets that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric. Every time a zone is added to a zoneset this constitutes a linkage.
- **MaxMembersPerZone is 2000**. The maximum number of zone members that can be added to any zone on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric. Aliases are considered zone members when added to a zone.
- **MaxMembersPerAlias is 2000**. The maximum number of zone members that can be added to any alias on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.

3.4.1.5
Zoning Configuration

You can set the FC-SW-2 Auto Save and Default Visibility zoning configuration parameters using SANbox Manager. The Auto Save parameter determines whether changes to the active zone set that a switch receives from another switch in the fabric will be saved to permanent memory on that switch. The Default

Visibility parameter permits or prohibits communication among ports/devices when there is no active zone set. Refer to ”Using the Zoning Config Dialog” on page 3-17 for information about zoning configuration using SANbox Manager.

3.4.2
Using the Zoning Config Dialog

Use the Zoning Config dialog to change the Auto Save and Default Visibility configuration parameters. In the faceplate display, open the Zoning menu and select **Edit Zoning Config** to open the Zoning Config dialog shown in Figure 3-5. After making changes, click the **OK** button to put the new values into effect.

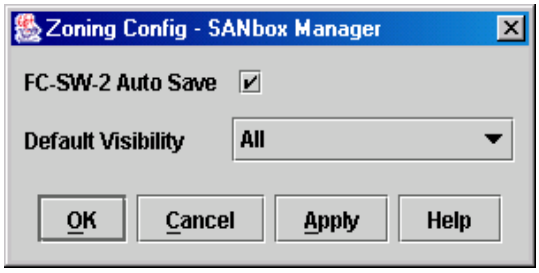


Figure 3-5. Zoning Config Dialog

3.4.2.1
FC-SW-2 Auto Save

The FC-SW-2 Auto Save parameter determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to the zoning database on that switch. Changes are saved when an updated zone set is activated. Zoning changes are always saved to temporary memory. However, if Auto Save is enabled, the switch firmware saves changes to the active zone set in temporary memory and to the zoning database. If Auto Save is disabled, changes to the active zone set are stored only in temporary memory which is cleared when the switch is reset.

3.4.2.2
Default Visibility

Default visibility determines the level of communication that is permitted among ports/devices when there is no active zone set. The default visibility parameter can be set differently on each switch. When default visibility is enabled (ALL) on a switch, all ports/devices on the switch can communicate with all ports/devices on switches that also have default visibility enabled. When Default Visibility is disabled (NONE), none of the ports/devices on that switch can communicate with any other port/device in the fabric.

3.4.3
Restoring Default Zoning

Restoring the default zoning clears the switch of all zoning definitions.

CAUTION! This command will deactivate the active zone set.

To restore the default zoning for a switch:

1. In the faceplate display, open the Zoning menu and select **Restore Default Zoning**.
2. Click the **OK** button to confirm that you want to restore default zoning and save changes to the zoning database.

3.4.4
Merging Fabrics and Zoning

If you join two fabrics with an inter-switch link, the active zone sets from the two fabrics attempt to merge automatically. The fabrics may consist of a single switch or many switches already connected together. The switches in the two fabrics attempt to create a new active zone set containing the union of each fabric's active zone set. The propagation of zoning information only affects the active zone set, not the configured zone sets, unless FC-SW-2 Auto Save is turned on.

3.4.4.1
Zone Merge Failure

If a zone merge is unsuccessful, the inter-switch links between the fabrics will isolate due to a zone merge failure, which will generate an alarm. The reason for the E_Port isolation can also be determined by viewing the port information. Refer to ”Port Information Data Window” on page 5-7 and the ”Show Command” on page A-53 (Port keyword).

A zone merge will fail if the two active zone sets have member zones with identical names that differ in membership or type. For example, consider Fabric A and Fabric B each with a soft zone named “ZN1” in its active zone set. Fabric A "ZN1" contains a member specified by Domain ID 1 and Port 1; Fabric B “ZN1” contains a member specified by Domain ID 1 and Port 2. In this case, the merge will fail because the two zones have the same name, but different membership.

3.4.4.2
Zone Merge Failure Recovery

When a zone merge failure occurs, the conflict that caused the failure must be resolved. You can correct a failure due to a zone conflict by deactivating one of the active zone sets or by editing the conflicting zones so that their membership is the same. You can deactivate the active zone set on one fabric if the active zone set on the other fabric accurately defines your zoning needs. If not, you must edit

the zone memberships, and reactivate the zone sets. After correcting the zone membership, reset the isolated ports to allow the fabrics to join.

Note: If you deactivate the active zone set in one fabric and the Auto Save parameter is enabled, the active zone set from the second fabric will propagate to the first fabric and replace all zones with matching names in the configured zone sets.

If the zone sets to merge have the same Zone A that only differ in the type of zone (soft vs. ACL), the zone sets will merge. If this is a 2 switch fabric, Switch 1 will state that Zone A is soft and Switch 2 will state that Zone A is ACL.

Refer to ”Managing Zones” on page 3-24 for information about adding and removing zone members. Refer to ”Resetting a Port” on page 5-16 for information about resetting a port.

3.4.5 Using the Edit Zoning Dialog

To edit the zoning database for a particular switch, open the Zoning menu from the faceplate display and select **Edit Zoning** to open the Edit Zoning dialog shown in Figure 3-6. Changes can only be made to inactive zone sets, which are stored in flash (non-volatile) memory and retained after resetting a switch.

To apply zoning to a fabric, choose a zone set and activate it. When you activate a zone set, the switch distributes that zone set and its zones, excluding aliases, to every switch in the fabric. This zone set is known as the active zone set.

You can not edit an active zone set on a switch. You must configure an inactive zone set to your needs and then activate that updated zone set to apply the changes to the fabric. When you activate a zone set, the switch distributes that zone set to the temporary zoning database on every switch in the fabric. However, in addition to the merged active zone set, each switch maintains its own original zone set in its zoning database. Only one zone set can be active at one time.

Note: If the FC-SW2-Auto-Save parameter is enabled on the Switch Properties dialog, then every time the active zone set changes, the switch will copy it into an inactive zone set stored on the switch. You can edit this copy of the active zone set stored on the switch, and activate the updated copy to conveniently apply the changes to the active zone set. The edited copy then becomes the active zone set.

The Edit Zoning dialog has a Zone Sets tree on the left and a Port/Device (or members) tree on the right. Both trees use display conventions similar to the fabric tree for expanding and contracting zone sets, zones, and ports. An

expanded port shows the port Fibre Channel address; an expanded address shows the port World Wide Name. You can select zone sets, zones, and ports in the following ways:

- Click a zone, zone set, or port icon.
- Right-click to select a zone set or zone, and open the corresponding popup menu.
- Hold down the Shift key while clicking several consecutive icons.
- Hold down the Control key while clicking several non-consecutive icons.

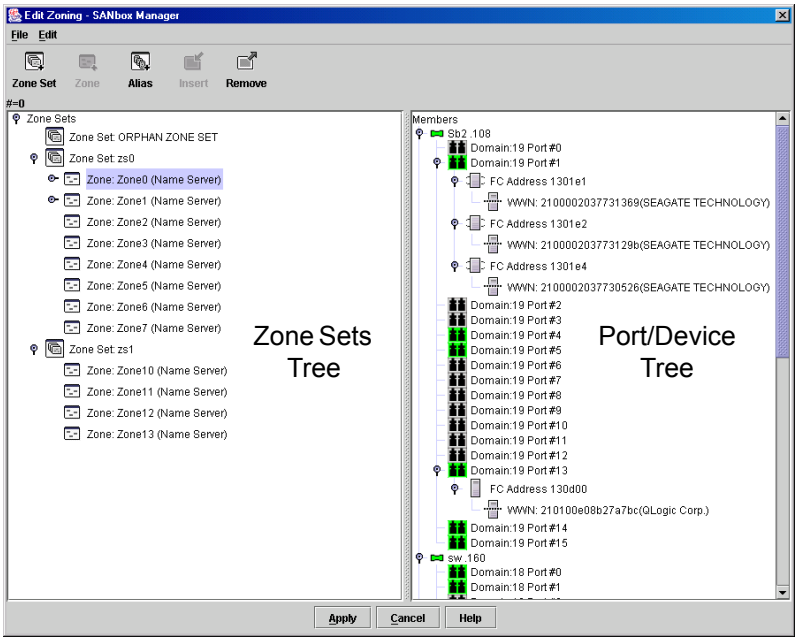


Figure 3-6. Edit Zoning Dialog

Using tool bar buttons, popup menus, or a drag-and-drop method, you can create and manage zone sets and zones in the zoning database. Table 3-3 describes the zoning tool bar operations.

Use the Edit Zoning dialog to define zoning changes, and click the **Apply** button to open the Error Check dialog. Click the **Error Check** button to have SANbox Manager check for zoning conflicts, such as empty zones, aliases, or zone sets, and ACL zones with non-domain ID/port number membership. Click the **Save Zoning** button to implement the changes. Click the **Close** button to close the Error Check dialog. On the Edit Zoning dialog, click the **Close** button to close the Edit Zoning dialog.

Table 3-3. Edit Zoning Dialog Tool Bar Buttons and Icons

Tool Bar Button	Description
	Create Zone Set button - create a new zone set
	Create Zone button - create a new zone
	Create Alias button - create another name for a set of objects
	Add Member button - add the selected zone to a zone set, or add the selected port/device to a zone
	Remove Member button - delete the selected zone from a zone set, or delete the selected port/device from a zone
	Switch port icon – not logged in
	Switch port icon – logged in
	NL_Port (loop) device icon – logged in to fabric
	NL_Port (loop) device icon – not logged in to fabric
	N_Port device icon – logged in to fabric
	N_Port device icon – not logged in to fabric

3.4.6
Managing Zone Sets

Zoning a fabric involves creating a zone set, creating zones as zone set members, then adding devices as zone members. The zoning database supports multiple zone sets to serve the different security and access needs of your storage area network, but only one zone set can be active at one time. Managing zone sets consists of the following tasks:

- Creating zone sets
- Activating and deactivating zone sets
- Copying a zone to a zone set
- Removing a zone from one zone set or from all zone sets
- Removing a zone set
- Removing all zoning definitions

Note: Changes that you make to the zoning database are limited to the managed switch and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switches.

3.4.6.1
Creating a Zone Set

To create a zone set, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Open the Edit menu, and select **Create Zone Set** to open the Create Zone Set dialog.
3. Enter a name for the zone set, and click the **OK** button. The new zone set name is displayed in the Zone Sets dialog. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, -, ^, and $.
4. To create new zones in a zone set, do one of the following:
   - Right-click a zone set and select **Create A Zone** from the popup menu. In the Create a Zone dialog, enter a name for the new zone, and click the **OK** button. The new zone name is displayed in the Zone Sets dialog.
   - Copy an existing zone by dragging a zone into the new zone set. Refer to ”Copying a Zone to a Zone Set” on page 3-23.
5. Click the **Apply** button to save changes to the zoning database.

3.4.6.2

Activating and Deactivating a Zone Set

You must activate a zone set to apply its zoning definitions to the fabric. Only one zone set can be active at one time. When you activate a zone set, the switch distributes that zone set to the temporary zoning database on every switch in the fabric.

The purpose of the deactivate function is to suspend all fabric zoning which results in free communication fabric wide or no communication depending on the default visibility setting. Refer to ”Default Visibility” on page 3-17 for more information. It is not necessary to deactivate the active zone set before activating a new one.

- To activate a zone set, open the Zoning menu and select **Activate Zone Set** to open the Activate Zone Set dialog. Select a zone set from the Select Zone Set pull-down menu, and click the **Activate** button.
- To deactivate the active zone set, open the Zoning menu, select **Deactivate Zone Set**. Acknowledge the warning about traffic disruption, and click the **Yes** button to confirm that you want to deactivate the active zone set.

3.4.6.3

Copying a Zone to a Zone Set

To copy an existing zone and its membership from one zone set to another, select the zone and drag it to the chosen zone set. Click the **Apply** button to save changes to the zoning database.

3.4.6.4

Removing a Zone from a Zone Set or from All Zone Sets

You can remove a zone from a zone set or from all zone sets in the database.

1. In the faceplate display, open the Zoning menu and select **Edit Zoning** to open the Edit Zoning dialog.
2. In the Zone Sets tree, select the zone(s) to be removed.
3. Open the Edit menu, and select **Remove** to remove the zone from the zone set, or select **Remove from All Zones** to remove the zone from all zone sets.
4. Click the **Apply** button to save changes to the zoning database.

Alternatively, you may use shortcut menus to remove a zone from a zone set or from all zone sets in the database.

3.4.6.5
Removing a Zone Set

Removing a zone set from the database affects the member zones in the following ways.

- Member zones that are members of other zone sets are not affected.
- Member zones that are not members of other zone sets become members of the orphan zone set. The orphan zone set is not saved on the switch.

To delete a zone set from the database, do the following:

1. In the faceplate display, open the Zoning menu and select **Edit Zoning** to open the Edit Zoning dialog.
2. In the Zone Sets tree, select the zone set to be removed.
3. Open the Edit menu, and select **Remove** to remove the zone set.
4. Click the **Apply** button to save changes to the zoning database.

Alternatively, you may use shortcut menus to remove a zone set from the database.

3.4.6.6
Removing All Zoning Definitions

To clear all zone and zone set definitions from the zoning database, choose one of the following:

- Open the Edit menu and select **Clear Zoning**. In the Removes All dialog, click the **Yes** button to confirm that you want to delete all zones and zone sets.
- Right-click the Zone Sets heading at the top of the Zone Sets tree, and select **Clear Zoning** from the popup menu. Click the **Yes** button to confirm that you want to delete all zone sets and zones.

3.4.7
Managing Zones

Managing zones involves the following:

- Creating a zone in a zone set
- Adding zone members
- Renaming a zone or a zone set
- Removing a zone member
- Removing a zone from a zone set
- Removing a zone from all zone sets
- Changing zone types
- Saving a zoning file

Note: Changes that you make to the zoning database are limited to the managed switch and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switches.

3.4.7.1

Creating a Zone in a Zone Set

When a zone is created, its zone type is soft. To change the zone type to a hard zone, refer to "Changing Zone Types" on page 3-28 for more information. Refer to "Zones" on page 3-14 for information on zone types (soft and hard). To create a zone in a zone set, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Select a zone set.
3. Open the Edit menu and select **Create a Zone**.
4. In the Create a Zone dialog, enter a name for the new zone, and click the **OK** button. The new zone name is displayed in the Zone Sets dialog. A zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, ^, $, and -.

   Note: If you enter the name of a zone that already exists in the database, the SANbox Manager application will ask if you would like to add that zone and its membership to the zone set.

5. To add switch ports or attached devices to the zone, do one of the following:
   - In the zone set tree, select the zone set. In the graphic window, select the port to add to the zone. Open the Edit menu and select **Add Members**.
   - Select a port by port number, Fibre Channel address, or World Wide Name in the Port/Device tree, and drag it into the zone.
   - Select a port by port number, Fibre Channel address, or World Wide Name in the Port/Device tree. Right-click the zone and select **Add Zone Members** from the popup menu.
6. Click the **Apply** button to save changes to the zoning database.

3.4.7.2
Adding Zone Members

Adding a zone member to a zone will affect every zone set in which that zone is a member. To add member ports/devices to a zone, do one of the following:

- Select a port by port number, Fibre Channel address, or World Wide Name in the Port/Device tree, and drag it into the zone. To select and drag multiple ports/devices, press and hold the Control key while dragging.
- Select one or more ports by port number, Fibre Channel address, or World Wide Name in the Port/Device tree. Right-click the zone and select **Add Zone Members** from the popup menu.
- Open the Edit menu or right click on the selected zone and select **Create Members**. Choose the WWN, Domain/Port, or First Port Address radio button and enter the port hex value.

Click the **Apply** button to save changes to the zoning database.

Note: Domain ID conflicts can result in automatic reassignment of switch domain IDs. These reassignments are not reflected in zones that use domain ID/port number pair to define their membership. Be sure to reconfigure zones that are affected by a domain ID change.

3.4.7.3
Creating a Member

The Create a Member dialog allows you to add a member to a zone or alias that can not be added using the drag/drop method. The Create a Member dialog must be used to add a domain/port member to a zone or alias from a non-QLogic switch.

To create a member, do the following:

1. In the faceplate display, click the **Zoning** button or open the Zoning menu and select **Edit Zoning**.
2. In the Edit Zoning dialog, select the zone or alias in the left pane in which to add a member.
3. Open the Edit menu and select **Create Members** to open the Create a Member dialog.
4. Click the **WWN**, **Domain Port**, or **FC Address** radio button.
5. Enter the hexadecimal value for the new zone member. Enter 16 digits for a WWN member, 4 digits for a Domain Port member (DDPP), or 6 digits for an FC Address member (DDPPAA - D=Domain ID, P=PortNumber, A=ALPA).
6. Click the **OK** button to add the member and save the change.

3.4.7.4

Renaming a Zone or a Zone Set

To rename a zone, do the following:

1. In the Zone Sets tree of the Edit Zoning dialog, click the zone/zone set to be renamed.
2. Open the Edit menu and select **Rename**.
3. In the Rename Zone/Rename Zone Set dialog, enter a new name for the zone/zone set.
4. Click the **OK** button.

3.4.7.5

Removing a Zone Member

Removing a zone member will affect every zone and zone set in which that zone is a member. To remove a member from a zone:

1. In the Edit Zoning dialog, select the zone member to be removed.
2. Open the Edit menu and select **Remove**.
3. Click the **OK** button to save changes and close the Edit Zoning dialog.

3.4.7.6

Removing a Zone from a Zone Set

Zones that are no longer members of any zone set are moved to the orphan zone set. The orphan zone set is saved on the switch. To remove a zone from a zone set, do the following:

1. In the Edit Zoning dialog, select the zone to be removed. The selected zone will be removed from that zone set only.
2. Open the Edit menu and select **Remove**.
3. Click the **OK** button to save changes and close the Edit Zoning dialog.

3.4.7.7

Removing a Zone from All Zone Sets

Zones that are no longer members of any zone set are moved to the orphan zone set. The orphan zone set is saved on the switch. To remove a zone from all zone sets including the orphan zone set, do the following:

1. In the Edit Zoning dialog, select the zone to be removed.
2. Open the Edit menu and select **Remove Zone from All Sets**.
3. Click the **OK** button to save changes and close the Edit Zoning dialog.

3.4.7.8
Changing Zone Types

To change a zone type, do the following:

1. In the faceplate display, select the switch with the zone type to change.
2. Click the **Zoning** button to open the Edit Zoning dialog.
3. In the Zone Sets tree, select the zone to change.
4. Open the Edit menu and select **Set Zone Type** to open the Set Zone Type dialog.
5. Open the Zone Type pull-down menu and select **Soft** or **ACL**.
   - Soft zoning is the least restrictive type of zoning.
   - ACL zoning is hard zoning and is enforced by hardware and defines access to a given port. ACL zones need not include inter-switch links.

3.4.8
Managing Aliases

An alias is a collection of objects that can be zoned together. An alias is not a zone, and can not have a zone or another alias as a member.

Note: Changes that you make to the zoning database are limited to the managed switch and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switches.

You will not see aliases in the active zone set.

3.4.8.1
Creating an Alias

To create an alias, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Open the Edit menu, and select **Create Alias** to open the Create Alias dialog.
3. Enter a name for the alias, and click the **OK** button. The alias name is displayed in the Zone Sets dialog. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -.
4. Click the **OK** button to save the alias name to the zoning database.

3.4.8.2

Adding a Member to an Alias

You can add a member to an alias in the following ways:

- Drag-and-drop method.
- Select the alias in the left pane and the member in the right pane to add to that alias, and click the **Insert** button.
- Select the alias in the left pane and the member in the right pane to add to that alias, and open the Edit menu and select **Add Members**.

To add a member to an alias using the drag-and-drop method, do the following:

1. In the right pane, click and hold down the mouse button on the member to be added to the alias.
2. Drag the selected member from the right pane to the alias in the left pane.

To add a member to an alias using the menu options, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. In the left pane, select an alias.
3. In the right pane, select the member to add to the selected alias.
4. Choose one of the following:
   - Open the Edit menu and select **Add Members**.
   - Click the **Insert** button.
5. Click the **OK** button to save changes and close the Edit Zoning dialog.

3.4.8.3

Removing an Alias from All Zones

To remove an alias from all zones, do the following:

1. In the Zone Sets tree in the Edit Zoning dialog, select the alias to be removed.
2. Open the Edit menu, and select **Remove Alias from All Zones**.
3. Click the **Yes** button in the Remove dialog.

3.4.9
Saving the Zoning Database to a File

You can save the zoning database to an XML file. You can later reload this zoning database on the same switch or another switch. To save a zoning database to a file, do the following:

1. In the faceplate display, open the Zoning menu, and select **Edit Zoning**.
2. In the Edit Zoning dialog, open the File menu and select **Save As**.
3. In the Save dialog, enter a file name for the database file.
4. Click the **Save** button to save the zoning file.

Section 4

Managing Switches

This section describes the following tasks that manage switches in the fabric.

- Managing user accounts
- Displaying switch information
- Configuring port threshold alarms
- Exporting name server information to a file
- Exporting FDMI information to a file
- Paging a switch
- Setting the date and time
- Setting temperature thresholds
- Resetting a switch
- Configuring a switch
- Archiving a switch
- Restoring a switch
- Restoring the factory default configuration
- Managing firmware
- Displaying hardware status

4.1 Managing User Accounts

Only the Admin account can manage user accounts with the User Account Administration dialogs. However, any user can modify their own password. To open the User Account Administration dialogs, open the Switch menu in the faceplate display, and select **User Accounts...**. A user account consists of the following:

- Account name or login
- Password
- Authority level
- Expiration date

Switches come from the factory with the following user accounts:

Table 4-1. Factory User Accounts

Account Name	Password	Admin Authority	Expiration
admin	admin	true	never expires
images	images	false	never expires

The Admin account is the only user that can manage all user accounts with the User Account Administration dialogs. The Admin account can create, remove, or modify user accounts, and change account passwords. The Admin account can also view and modify the switch and its configuration with SANbox Manager. The Admin account can not be removed.

Users with Admin authority can view and modify the switch and its configuration using SANbox Manager. Users without Admin authority are limited to viewing switch status and configuration.

The Images account can not be removed, and is required for exchanging files with the switch using FTP.

The factory switch configuration does not enforce user accounts and passwords. This means that no account name and password are required to add a fabric and modify switch configurations using SANbox Manager. You can only use the command line interface to change the enforcement (on or off) of user accounts and authority. To enforce user accounts and authority, set the UserAuthentication parameter to True using the Set Setup System command. Refer to ”Set Setup Command” on page A-48.

4.1.1
Creating User Accounts

To create a user account on a switch, open the Switch menu in the faceplate display and select **User Accounts...**. This displays the User Account Administration dialog shown in Figure 4-1. A switch can have a maximum of 15 user accounts.

Figure 4-1. User Account Administration Dialog – Add Account

1. To open the User Account Administration dialogs, open the Switch menu in the faceplate display, and select **User Accounts...**.
2. Click the **Add Account** tab to open the Add Account tab page.
3. Enter an account name in the New Account Login field. Account names are limited to 15 characters.
4. If the account is to have the ability to modify switch configurations, check the **Admin Authority Enabled** box.
5. Enter a password in the New Password field and enter it again in the Verify Password field. A password must have a minimum of 4 characters and no more than 20.
6. If this account is to be permanent with no expiration date, click the **Permanent Account** radio button. Otherwise, click the **Account Will Expire** button and enter the number days in which the account will expire.
7. Click the **Add Account** button to add the newly defined account.

4.1.2
Removing a User Account

To remove a user account on a switch, open the Switch menu in the faceplate display and select **User Accounts...**. Click the **Remove Account** tab in the dialog to present the display shown in Figure 4-2. Select the account name from the list of accounts at the top of the dialog and click the **Remove Account** button.

Figure 4-2. User Account Administration Dialog – Remove Account

4.1.3

Changing a User Account Password

To change the password for an account on a switch, open the Switch menu in the faceplate display and select **User Accounts...**. Click the **Change Password** tab in the dialog to present the display shown in Figure 4-3. Select the account name from the list of accounts at the top of the dialog, then enter the old password, the new password, and verify the new password in the corresponding fields. Click the **Change Password** button. Any user can change their password for their account, but only the Admin account name can change the password for another user's account. If the administrator does not know the user's original password, the administrator must remove the account and add the account.

Figure 4-3. User Account Administration Dialog– Change Password

4.1.4
Modifying a User Account

To modify a user account on a switch, open the Switch menu in the faceplate display and select **User Accounts...**. This displays the User Account Administration dialog shown in Figure 4-4. Click the **Modify Account** tab. Select the account name from the list of accounts at the top of the dialog. Click the Admin authority Enabled check box to grant admin authority to the account name. Click an Account Expiration Date radio button. If the account is not to be permanent, enter the number of days until the account expires. Click the **Modify Account** button to save the changes. Click the **Close** button to close the User Account Administration dialog.

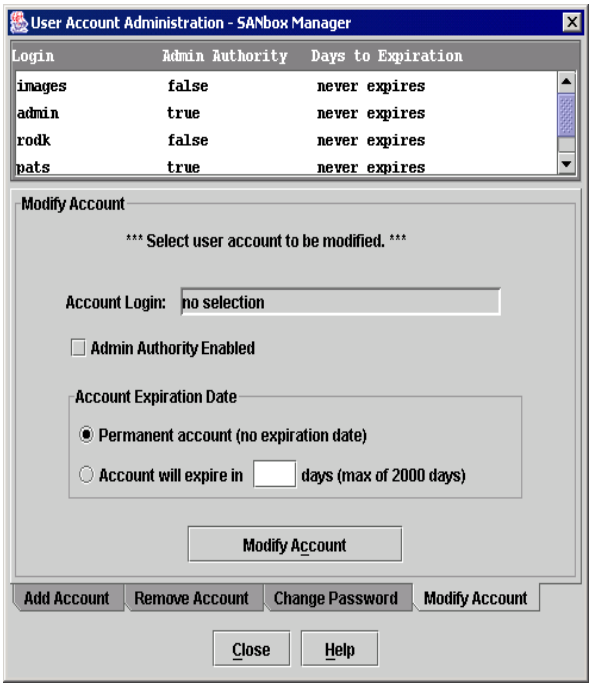


Figure 4-4. User Account Administration Dialog – Modify Account

4.2 Displaying Switch Information

The faceplate display and data windows provide the following switch information:

- Name server information
- Device and HBA information
- Switch specifications and addresses
- Configuration parameters
- Performance statistics
- Port information
- Configured zone sets

Figure 4-5 shows the faceplate display for the SANbox2-8c and SANbox2-16 switches.

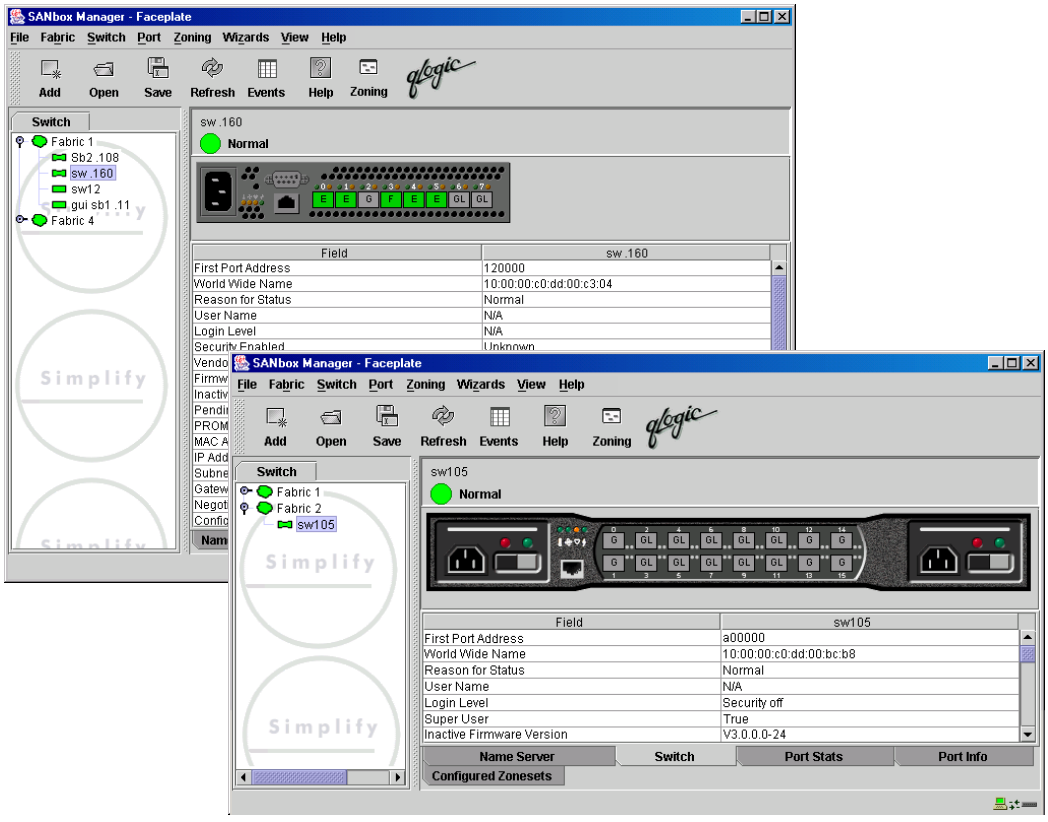


Figure 4-5. Faceplate Display

The fabric updates the topology and faceplate displays by forwarding changes in status to the management workstation as they occur. You can allow the fabric to update the switch status, or you can refresh the display at any time. To refresh switch status in the display, do one of the following:

- Click the **Refresh** button.
- Open the View menu and select **Refresh**.
- Press the F5 key.
- Right-click a switch in the topology display and select **Refresh Switch** from the popup menu.
- Right-click in the graphic window of the faceplate display, and select **Refresh Switch** from the popup menu.

4.2.1 Name Server Data Window

The Name Server data window displays information about the devices that are logged into the fabric. Click the **Name Server** tab below the data window to display name server information for all devices that are logged into the selected fabric. To narrow the display to devices that are logged into specific switches, select one or more switches in the fabric tree or the topology display. Refer to Table 4-2 for a description of the entries in the Name Server data window. Refer to ”Exporting Name Server Information to a File” on page 4-17 for exporting name server information.

Table 4-2. Name Server Data Window Entries

Entry	Description
Target/Initiator	Device type: target or initiator
Switch	Switch name
Port	Switch port number
Address	Fibre Channel address
Type	Node type
WWNN	Node World Wide Name
WWPN	Port World Wide Name
Vendor	Host Bus Adapter/Device Vendor
FC-4 Types	Device Fibre Channel protocol types
Active Zones	The active zone to which the device belongs

4.2.2
FDMI Data Window

The FDMI data window displays device information from the fabric and allows devices to register certain information with the fabric. To open the FDMI data window, open the topology display and click the **FDMI** tab below the window. SANbox Manager will report any and all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch. To view FDMI data, FDMI must be enabled on the entry switch and on all other switches in the fabric which are to report FDMI data. To enable FDMI, select a switch in the topology display or open the faceplate display, open the Switch menu, select Switch Properties, and click the **Enable FDMI** radio button in the Switch Properties dialog.

Table 4-3. FDMI Data Window Entries

Entry	Description
HBA WWN	HBA World Wide Name
Details	Detail device information. Click the Information (i) button to open the Detailed FDMI Display dialog. Refer to ”Detailed FDMI Display Dialog” on page 4-10 for detailed FDMI information.
Vendor	Device vendor
Model	Device model
Node WWN	Node World Wide Name
H/W Version	Version of hardware
Driver Version	Version of driver software
F/W Version	Version of firmware
OS	Operating System used
# Ports	Number of device ports

The Detailed FDMI Display dialog is opened after clicking the Information (i) button in the Details column of the FDMI data window, and lists additional FDMI information for the device. To open the FDMI data window, open the topology display and click the **FDMI** data window tab.

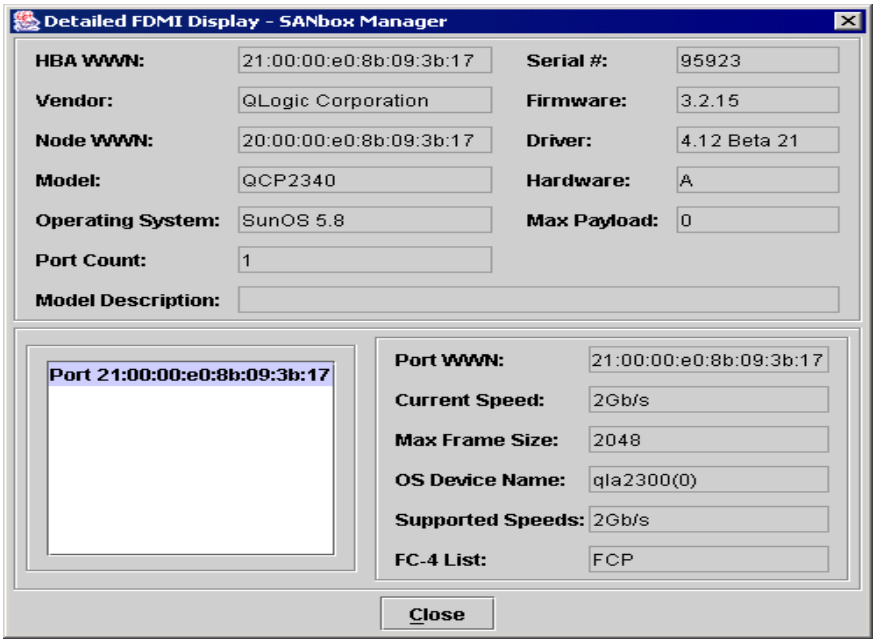


Figure 4-6. Detailed FDMI Display Dialog

4.2.3 Switch Data Window

The Switch data window displays current network and switch information for the selected switches. Refer to "Configuring a Switch" on page 4-20 for more information about the Switch data window. To open the Switch data window, select one or more switches in the topology display or open the faceplate display, and click the **Switch** tab below the window. Table 4-4 describes the Switch data window entries.

Table 4-4. Switch Data Window Entries

Entry	Description
First Port Address	Switch Fibre Channel address
World Wide Name	Switch World Wide Name
Serial Number	Number assigned to each chassis.
Reason for Status	Additional status information
User Name	Account name
Login Level	Authority level
Super User	Super user privileges enabled/disabled

Table 4-4. Switch Data Window Entries (Continued)

Entry	Description
UserAuthentication Enabled	Enforcement of account names and authority
Vendor	Switch manufacturer
Firmware Version	Active firmware version
Inactive Firmware Version	Inactive firmware version
Pending Firmware Version	Firmware version that will be activated at the next reset
PROM/Flasher Version	PROM firmware version
MAC Address	Media Access Control address
IP Address	Internet Protocol address
Subnet Mask	Mask that determines the IP address subnet
Gateway	Gateway address
SNMP Enabled	SNMP enabled or disabled.
Negotiated Domain ID	The domain ID currently being used by the fabric
Configured Domain ID	The domain ID defined by network administrator
Domain ID Lock	Domain ID lock status. Prevents (True) or permits (False) dynamic domain ID reassignment.
Number of Ports	Number of ports activated on the switch
Switch Type	Switch model
Operational State	Switch operational state: Online, Offline, Diagnostic
Administrative State	Current switch administrative state
Configured Admin State	Switch administrative state that is stored in the switch configuration
R_A_TOV	Resource allocation timeout value
E_D_TOV	Error detect timeout value
FC-SW-2 Compliant	Zoning merge status. If True, changes to the active zone set are propagated throughout the fabric. If false, changes to both the active zone set and zoning database are propagated throughout the fabric. Refer to the QLogic Switch Interoperability Guide found on the QLogic Web site.

Table 4-4. Switch Data Window Entries (Continued)

Entry	Description
Legacy Address Format	Legacy port addressing status. Enabled only for interoperability with non-FC-SW-2 switches.
FC-SW-2 Auto Save	Zoning auto save status. Saves zoning updates in temporary memory and the zoning database (True) or only in temporary memory (False).
Zoning Default Visibility	Zoning visibility status. Permits (All) or prevents (None) communication between attached devices in the absence of an active zone set.
Temperature	Internal switch temperature °C
Security Auto Save	N/A
Security Fabric Binding Enable	N/A
Fan 1 Status	Fan 1 status
Fan 2 Status	Fan 2 status (SANbox2-16 only)
Fan 3 Status	Fan 3 status (SANbox2-16 only)
Power Supply 1 Status	Power supply 1 status
Power Supply 2 Status	Power supply 2 status (SANbox2-16 only)
Beacon Status	Beacon status. Switch LEDs are blinking (On) or not (off).
Broadcast Support	Broadcast support status. Broadcast support is enabled or disabled (default).
In-band Enabled	In-band management status. Permits (True) or prevents (False) a switch from being managed over an ISL.
Temp Failure Port Shutdown	Port shutdown status. If True, all ports are downed when the switch temperature exceeds the Failure Temperature. If False (default), port operational states remain unchanged.
Warning Temperature	Warning temperature threshold in °C above which a warning condition alarm is generated and the sent to the event browser.
Failure Temperature	The temperature at which the ports will shutdown if Temp Failure PortShutdown is Enabled. If this option is disabled, the Event Browser will report a failure.

Table 4-4. Switch Data Window Entries (Continued)

Entry	Description
FDMI Enable	Fabric Device Management Interface status. If enabled, device information can be obtained, managed, and saved through the fabric using Name Service Management Server functions. SANbox Manager will report any and all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch.
FDMI HBA Entry Limit	Maximum number of HBAs that can be registered with a switch.
Number of Donor Groups	Total number of donor port groups. A donor group is a set of ports on a switch that can donate buffer credits to each other.

4.2.4
Link Data Window

The Link data window displays information about all switch links in the fabric or selected links. This information includes the switch name, the port number at the end of each link, and the link status. To open the Link data window, click the **Link** tab below the data window in the topology display.

4.2.5
Port Statistics Data Window

The Port Statistics data window displays port performance data for the selected ports. To open the Port Statistics data window, click the **Port Stats** tab below the data window in the faceplate display. Refer to Table 5-5 for a description of the Port Statistics data window entries.

The Statistics pull-down menu is available on the Port Statistics data window, and provides different ways to view detailed port information. Click the down arrow to open the pull-down menu. Open the pull-down menu and select **Absolute** to view the total count of statistics since the last switch reset. Select **Rate** to view the number of statistics counted per second over the polling period. Select **Baseline** to view the total count of statistics since the last time the baseline was set. Click the **Clear Baseline** button to set the current baseline.

4.2.6
Port Information Data Window

The Port Information data window displays port detail information for the selected ports. To open the Port Statistics data window, click the **Port Info** tab below the data window in the faceplate display. Refer to Table 5-6 for a description of the Port Information data window entries.

4.2.7
Configured and Active Zonesets Data Windows

The Configured Zonesets data window displays all zone sets, zones, aliases, and zone membership in the zoning database, as shown in Figure 4-7. To open the Configured Zonesets data window, click the **Configured Zonesets** tab below the data window in the faceplate display. To view the active zonesets in the Active Zonesets data window, open the topology display and click the **Active Zonesets** data window tab.

The Configured Zonesets data window uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded. Click this handle or double-click the following entries to expand or collapse them:

- A zone set entry expands to show its member zones.
- A zone entry expands to show its members by port number, World Wide Name, or Fibre Channel address.
- The alias entry expands to show its entries.

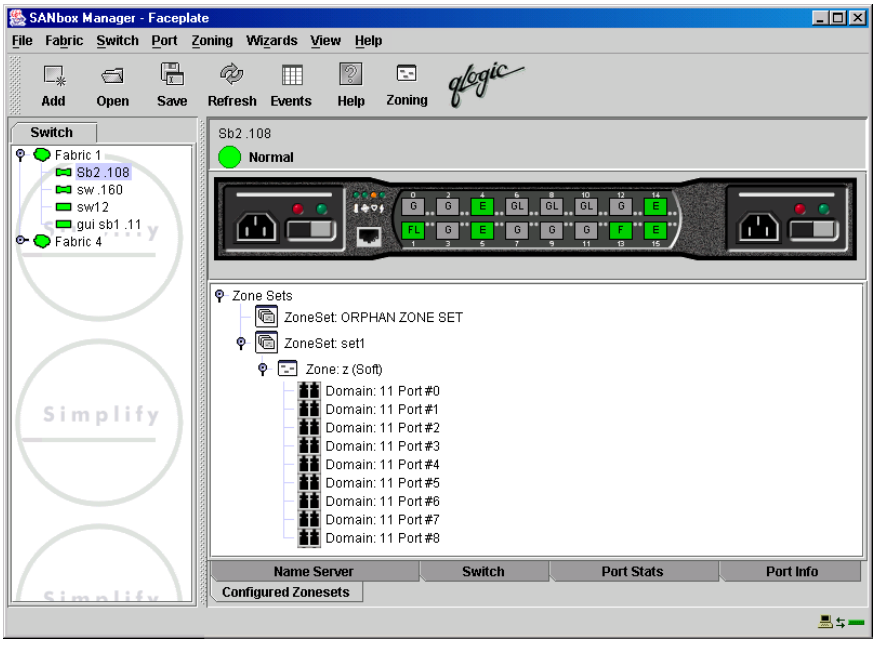


Figure 4-7. Configured Zonesets Data Window

4.3

Configuring Port Threshold Alarms

You can configure the switch to generate alarms for selected events. Configuring an alarm involves choosing an event type, rising and falling triggers, a sample window, and finally enabling or disabling the alarm. To configure port threshold alarms, do the following:

1. In the faceplate display, open the Switch menu and select **Port Threshold Alarm Configuration**. The Port Threshold Alarm Configuration dialog shown in Figure 4-8 prompts you to enable or disable all alarms, select an event, set triggers, set a sample window and enable or disable an individual alarm.

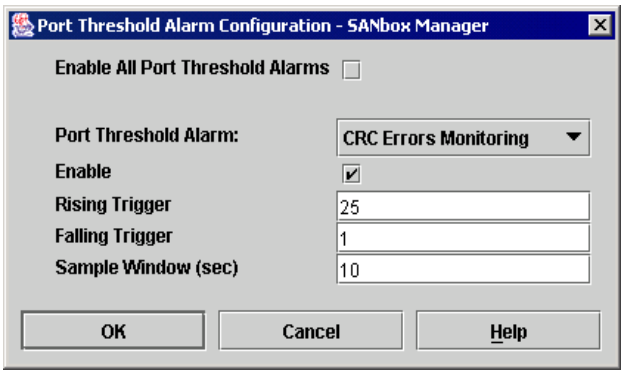


Figure 4-8. Port Threshold Alarm Configuration Dialog

2. Check the **Enable All Port Threshold Alarms** check box to enable monitoring for all the individual alarm types that are enabled. The **Enable All Port Threshold Alarms** check box is the master control for the individual alarms. For example, the switch will monitor CRC errors only if both the CRC Error **Enable** box and the **Enable All Port Threshold Alarms** box are checked.
3. Select an event type from the Port Threshold Alarm pull-down menu. Choose from the following options:
   - CRC error monitoring
   - Decode error monitoring
   - ISL monitoring
   - Login monitoring
   - Logout monitoring
   - Loss of signal monitoring
4. Check the **Enable** box to make the alarm eligible for use.

5. Enter a value for the rising trigger. A rising trigger alarm is generated when the event count per interval exceeds the rising trigger. The switch will not generate another rising trigger alarm for that event until the count descends below the falling trigger and rises again above the rising trigger. Consider the example in Figure 4-9.
6. Enter a value for the falling trigger. A falling trigger alarm is generated when the event count per interval descends below the falling trigger.

Note: The switch will down a port if a rising trigger alarm is not cleared after three consecutive sample windows.

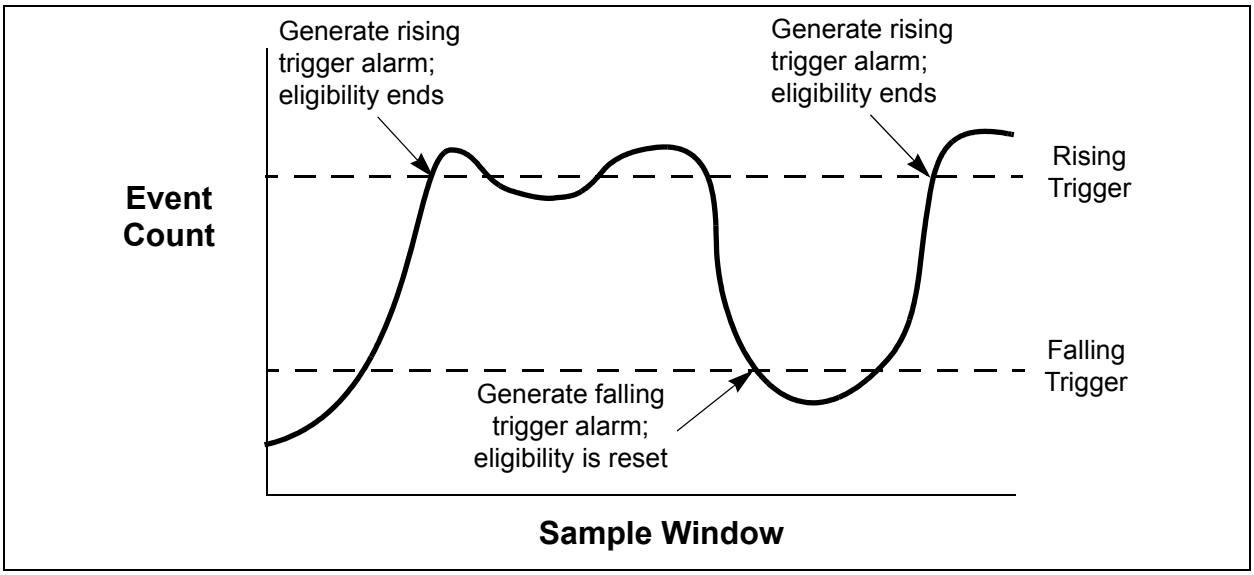


Figure 4-9. Port Threshold Alarm Example

7. Enter a sample window in seconds. The sample window defines the period of time in which to count events.
8. Repeat steps 3 through 7 for each alarm you want to configure or enable.
9. Click the **OK** button to save all changes.

4.4
Exporting Name Server Information to a File

To save name server information to a file, open the topology display and do the following:

1. Select one or more switches. If no switches are selected, name server information is gathered for all switches.
2. Open the Switch menu and select **Export Name Server**.
3. In the Save dialog, enter a file name.
4. Click the **Save** button.

4.5
Exporting FDMI Information to a File

SANbox Manager will report any and all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch. To save FDMI information to a file, do the following:

1. Open the topology display.
2. Open the Switch menu and select **Export FDMI**.
3. In the Save dialog, enter a file name.
4. Click the **Save** button.

4.6
Paging a Switch

You can use the beacon feature to page a switch. The beacon feature causes all Logged-In LEDs to flash, making it easier to recognize. To page a switch, open the Switch menu in the faceplate display and enable the **Toggle Beacon** selection. To cancel the beacon, reselect **Toggle Beacon**.

4.7
Setting the Date and Time

To set the date and time on a switch, do the following:

1. Select a switch in the topology display, and open the faceplate display.
2. Open the Switch menu, and select **Set Date/Time...**.
3. Enter the year, month, day and time in the Switch Date and Time dialog, then click **OK**. The new date and time take effect immediately.

4.8

Setting Temperature Thresholds

You can set temperature thresholds by which the switch will generate an alarm or place the switch offline. The Temperature Thresholds dialog shown in Figure 4-10 prompts you to enter a warning threshold and a failure threshold temperature (°C). To open the Temperature Thresholds dialog, open the faceplate display, open the Switch menu and select **Temperature Thresholds...**

- If the switch internal temperature exceeds the warning threshold, the switch generates an alarm.
- If the switch internal temperature exceeds the failure threshold and the **Enable Temperature Failure Port Shutdown** box is checked, the switch generates an alarm and places all ports down. After correcting the problem, you must reset the switch to bring the ports back online.

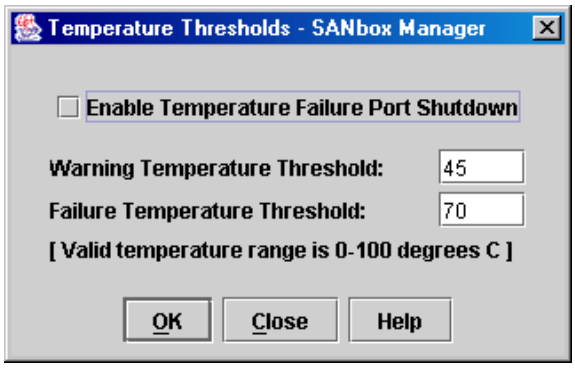


Figure 4-10. Temperature Thresholds Dialog

4.9

Resetting a Switch

Resetting a switch reboots the switch using configuration parameters in memory. Depending on the reset type, a switch reset may or may not include a power-on self test or it may or may not disrupt traffic. Table 4-5 describes the types of switch resets.

During a hotreset operation, fabric services will be unavailable for a short period (30-75 seconds depending on switch model). To ensure that an NDCLA operation is successful, verify that all administrative changes to the fabric (if any) are complete. When upgrading firmware across a fabric using non-disruptive activation, upgrade one switch at a time and allow 75 seconds between switches.

CAUTION! Changes to the fabric may disrupt the NDCLA process.

Common administrative operations that change the fabric include:

- Zoning modifications.
- Adding, moving or removing devices attached to the switch fabric. This includes powering up or powering down attached devices.
- Adding, moving or removing ISLs or other connections.

Management Interfaces:

After an NDCLA operation is complete, management connections must be re-initiated:

- SANbox Manager sessions will re-connect automatically.
- Telnet sessions must be restarted manually.

Applicable Code Versions:

- NDCLA capability is available starting with version 2.0 of the switch code.
- Upgrading to version 2.0 from previous releases will be disruptive.
- Future switch code releases will be upgraded non-disruptively unless specifically indicated in its associated release notes.
- An NDCLA operation to previous switch code releases is not supported.

Table 4-5. Switch Resets

Type	Description
Hot Reset	Resets a switch without a power-on self test. This reset activates the pending firmware, but does not disrupt switch traffic. If errors are detected on a port during a hot reset, the port is reset automatically.
Reset without POST	Resets a switch without a power-on self test. This reset activates the pending firmware and it is disruptive to switch traffic.
Hard Reset	Resets a switch with a power-on self test. This reset activates the pending firmware and it is disruptive to switch traffic.

To reset a switch using SANbox Manager, do the following:

1. Select the switch to be reset and open the faceplate display.
2. Open the Switch menu and select the **Reset Switch** pull-down menu:
   - Select **Hot Reset** to perform a hot reset.
   - Select **Reset** to perform a standard reset.
   - Select **Hard Reset** to perform a hard reset.

4.10 Configuring a Switch

Switch configuration is divided into two areas: chassis configuration and network configuration. Chassis configuration specifies switch-wide Fibre Channel settings. Network configuration specifies Ethernet and SNMP settings.

To open the Switch Properties dialog, either select a switch in the topology display or open the faceplate display for the switch you will be configuring, and then open the Switch menu and select **Switch Properties**. You may also right-click a switch graphic in the topology display or faceplate display, and select **Switch Properties** from the popup menu.

4.10.1
Using the Configuration Wizard

The Configuration Wizard is a series of dialogs you can use to configure the IP address and other basic parameters on new or replacement switches. SANbox Manager will detect the first time use and present the Initial Start dialog, from which the Configuration Wizard can be launched. The Configuration Wizard allows you to assign a temporary IP address to a connected switch, eliminating the need to change your workstation's IP address for initial configuration of a new switch. You can also launch the Configuration Wizard from the Wizards menu in either the topology display or the faceplate display. Open the Wizards menu and select **Configuration Wizard**.

Use the Configuration Wizard to:

- Configure a new switch in a fabric.
- Add a new switch to an existing fabric.
- Replace or restore a switch in an existing fabric.
- Recover or edit the IP configuration of an existing switch.

4.10.2
Switch Properties

Use the Switch Properties dialog to change the following switch configuration parameters:

- Symbolic name
- Administrative state
- Domain ID and domain ID lock
- FDMI and FDMI HBA entry limit
- Broadcast support (TCP/IP)
- In-band management
- FC-SW-2 compliance for zoning
- Legacy port address format

The timeout values are displayed only for reference purposes when the switch is online; they become active when the switch is taken offline. After making changes, click the **OK** button to put the new values into effect.

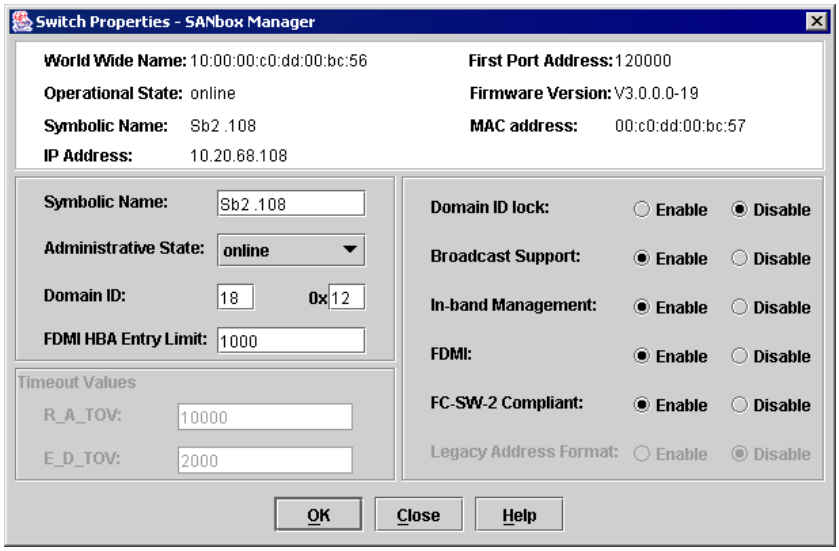


Figure 4-11. Switch Properties Dialog

4.10.2.1
Symbolic Name

The symbolic name is a user-defined name of up to 63 characters that identifies the switch. The symbolic name is used in the topology and faceplate displays, as well as many data windows to more easily identify switches. The illegal characters are the pound sign (#), semi-colon (;), and comma (,).

4.10.2.2
Switch Administrative States

The switch administrative state determines the operational state of the switch. The switch administrative state exists in two forms: the configured administrative state and the current administrative state.

- The configured administrative state is the state that is saved in the switch configuration and is preserved across switch resets. SANbox Manager always makes changes to the configured administrative state. The configured administrative state is displayed in the Switch Properties dialog.
- The current administrative state is the state that is applied to the switch for temporary purposes and is not retained across switch resets. The current administrative state is set using the Set Switch command. Refer to the ”Set Command” on page A-30.

Table 4-6 describes the administrative state values.

Table 4-6. Switch Administrative States

Parameter	Description
Online	The switch is available.
Offline	The switch is unavailable.
Diagnostics	The switch is in diagnostics mode, is unavailable, and tests can then be run on all ports of the switch.

4.10.2.3
Domain ID and Domain ID Lock

The domain ID is a unique Fibre Channel identifier for the switch. The Fibre Channel address consists of the domain ID, port ID, and the Arbitrated Loop Physical Address (ALPA). The maximum number of switches within a fabric is 239 with each switch having a unique domain ID.

Switches come from the factory with the domain IDs unlocked. This means that if there is a domain ID conflict in the fabric, the switch with the highest principal priority, or the principal switch, will reassign any domain ID conflicts and establish the fabric. If you lock the domain ID on a switch and a domain ID conflict occurs, one of the switches will isolate as a separate fabric and the Logged-In LEDs on both switches will flash to show the affected ports. Refer to the ”Set Config Command” on page A-32 for information about the switch keyword and the Domain ID Lock and Principal Priority parameters.

If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain conflict occurs, the new switch will isolate as a separate fabric. However, you can remedy this by resetting the new switch or taking it offline then back online. The principal switch will reassign the domain ID and the switch will join the fabric.

Note: Domain ID reassignment is not reflected in zoning that is defined by domain ID and port number pair. You must reconfigure zones that are affected by domain ID reassignment.

4.10.2.4
Fabric Device Management Interface

Fabric Device Management Interface (FDMI) provides a means to gather and display device information from the fabric, and allows FDMI capable devices to register certain information with the fabric, if FDMI is enabled. SANbox Manager will report any and all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch. To view FDMI data, FDMI must be enabled on the entry switch and on all other switches in the fabric which are to report FDMI data.

FDMI is comprised of the fabric-to-device interface and the application-to-fabric interface. The fabric-to-device interface enables a device's management information to be registered. The application-to-fabric interface provides the framework by which an application obtains device information from the fabric. Use the **FDMI HBA Entry Limit** field on the Switch Properties dialog to configure the maximum number of HBAs that can be registered with a switch. If the number of HBAs exceeds the maximum number, the FDMI information for those HBAs can not be registered.

Use the **FDMI Enabled** radio button on the Switch Properties dialog to enable or disable FDMI. If FDMI is enabled on an HBA, the HBA forwards information about itself to the switch when the HBA logs into the switch. If FDMI is enabled on a switch, the switch stores the HBA information in its FDMI database. Disabling FDMI on a switch clears the FDMI database. If you disable FDMI on a switch, then re-enable it, you must reset the ports to cause the HBAs to log in again, and thus forward HBA information to the switch.

To view detailed FDMI information for a device, open the topology display, click the **FDMI** tab, and click the **Information (i)** button in the Details column of the FDMI data window. The Detailed FDMI Display dialog displays the specific information for that device. Refer to "FDMI Data Window" on page 4-9 for more information.

4.10.2.5
Broadcast Support

Broadcast is supported on the SANbox2 which allows for TCP/IP support. Broadcast is implemented using the proposed standard specified in *Multi-Switch Broadcast for FC-SW-3, T11 Presentation Number T11/02-031v0*. Fabric Shortest Path First (FSPF) is used to set up a fabric spanning tree used in transmission of broadcast frames. Broadcast frames are retransmitted on all ISLs indicated in the spanning tree and all online F_Ports. Broadcast zoning is supported with Access Control List (ACL) hard zones. When a broadcast frame is received, these hard zones are enforced at the F_Port. If the originator of the broadcast is in a hard zone, the frame is retransmitted on all online F_Ports within the hard zone. If the originator of the broadcast frame is not in a hard zone, the frame is retransmitted on online F_Ports that are not in a hard zone. The default setting is disabled.

4.10.2.6
In-band Management

In-band management is the ability to manage switches across inter-switch links using SANbox Manager, SNMP, management server, or the application programming interface. The switch comes from the factory with in-band management enabled. If you disable in-band management on a particular switch, you can no longer communicate with that switch by means other than a direct Ethernet or serial connection.

4.10.2.7
FC-SW-2 Compliance for Zoning

When a zone set is activated, SANbox2 switches and other FC-SW-2 compliant switches propagate the active zone set to all switches in the fabric. Some non-FC-SW-2 compliant switches propagate not only the active zone set, but the entire zoning database. Disabling this parameter causes the SANbox2 switch to propagate the zoning database, and therefore, interoperate with non-FC-SW-2 switches. For FC-SW-2 compliant fabrics, this parameter should be enabled.

Note: The **FC-SW-2 Compliant** setting must be the same on all switches in the fabric, otherwise the inter-switch links will not connect.

4.10.2.8
Legacy Port Address Format

Legacy Address Format should be enabled only to permit interoperation with certain older non-FC-SW-2 switches. Enabling this setting under other circumstances will disable zoning that is defined by domain ID and port number. This setting is available only when the **FC-SW-2 Compliant** setting is disabled. Contact your authorized maintenance provider for assistance in using this feature. Refer to the QLogic Switch Interoperability Guide on the QLogic Web site for a complete discussion of configuring for operation with non-Qlogic Switches.

Note: The **Legacy Address Format** setting must be the same on all switches in the fabric, otherwise the inter-switch links will not connect.

4.10.2.9
Timeout Values

The switch timeout values determine the timeout values for all ports on the switch. Table 4-7 describes the switch timeout parameters. The timeout values must be the same for all switches in the fabric.

Note: Mismatched timeout values will disrupt the fabric. These should not be changed unless absolutely necessary. Therefore, the switch must be offline to change these values. Use the Switch Properties dialog to take the switch offline.

Table 4-7. Timeout Values

Parameter	Description
R_A_TOV	Resource Allocation Timeout: Represents the maximum time a frame could be delayed in the Fabric and still be delivered. The default is 10000 milliseconds.
E_D_TOV	Error Detect Timeout: Represents the maximum round trip time that an operation between two N_Ports could require. The default is 2000 milliseconds.

4.10.3 Network Properties

Use the Network Properties dialog shown in Figure 4-12 to change IP and SNMP configuration parameters. After making changes, click the **OK** button to put the new values into effect. To open the Network Properties dialog, select a switch in the topology display or open the faceplate display, open the Switch menu and select **Network Properties**.

Note: Since Read Community, Trap Community, and Write Community settings are like passwords, they are write-only fields; the current settings are not displayed.

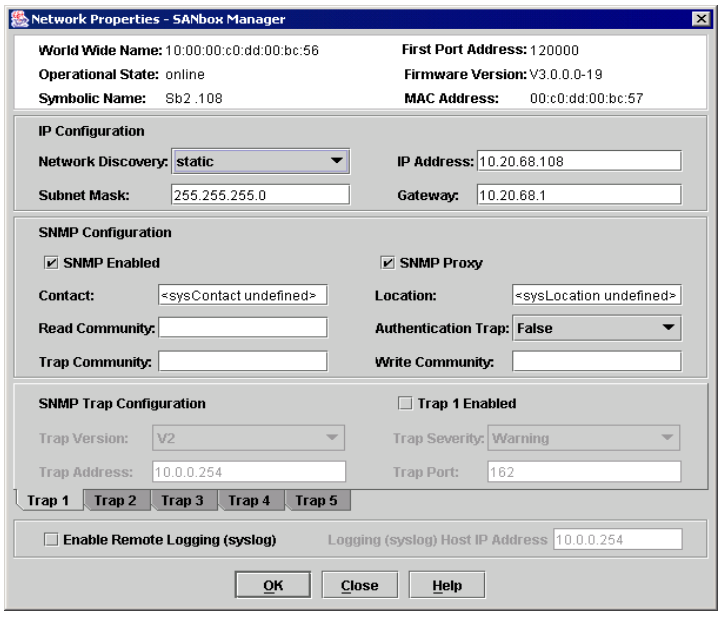


Figure 4-12. Network Properties Dialog

4.10.3.1

IP Configuration

The IP configuration identifies the switch on the Ethernet network and determines which network discovery method to use. Table 4-8 describes the IP configuration parameters.

Table 4-8. IP Configuration Parameters

Parameter	Description
Network Discovery	Choose one of the following methods by which to assign the IP address: ■ Static - Uses the IP configuration parameters entered in the Switch Properties dialog. ■ BootP - Acquires the IP configuration from a BootP server. ■ RARP (Reverse Address Resolution Protocol) - Acquires the IP address from an RARP server. An RARP request is broadcast with up to three retries, each at 5 second intervals. If no IP address is obtained, the switch reverts to the previously configured IP address. ■ DHCP (Dynamic Host Configuration Protocol) - Acquires the IP configuration from a DHCP server. If no satisfactory lease is obtained, the DHCP client attempts to use the previously configured lease. If the previous lease cannot be used, no IP address will be assigned to this switch in order to avoid an IP address conflict. The DHCP server must then be made available. If a BootP, RARP, or DHCP server is not available, the switch will attempt to use a previously assigned valid lease. If no lease was ever assigned, the switch will attempt to use the previously assigned static IP address.
IP Address	Internet Protocol (IP) address for the Ethernet port. The default value is 10.0.0.1.
Subnet mask	Subnet mask address for the Ethernet port. The default value is 255.0.0.0.
Gateway	IP gateway address. The default value is 10.0.0.254.

4.10.3.2

SNMP Configuration

The SNMP configuration defines how authentication traps are managed.Table 4-9 describes the SNMP configuration parameters. The illegal characters for the user-defined fields are the pound sign (#), semi-colon (;), and comma (,).

Table 4-9. SNMP Configuration Parameters

Parameter	Description
SNMP Enabled	Enables or disables SNMP communication with other switches in the fabric.
Contact	Specifies the name (up to 64 characters) of the person who is to be contacted to respond to trap events. The default is “undefined”.
Read Community	Read community password (up to 32 characters) that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “public”.
Trap Community	Trap community password (up to 32 characters) that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “public”.
SNMP Proxy	If enabled, you can use SNMP to monitor and configure any switch in the fabric.
Location	Specifies the name (up to 64 characters) for the switch location. The default is “undefined”.
Authentication Trap	Enables or disables the reporting of SNMP authentication failures. If enabled, a notification trap is sent when incorrect community string values are used. The default value is False.
Write Community	Write community password (up to 32 characters) that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “private”.

4.10.3.3
SNMP Trap Configuration

The SNMP trap configuration defines how traps are set. Choose from the tabs **Trap1** – **Trap 5** to configure each trap. Table 4-10 describes the SNMP configuration parameters.

Table 4-10. SNMP Trap Configuration Parameters

Parameter	Description
Trap Version	Specifies the SNMP version (1 or 2) with which to format traps.
Trap 1 Enabled	Enables or disables the trap. If disabled, traps are not configurable.
Trap Address[1]	Specifies the IP address to which SNMP traps are sent. A maximum of 5 trap addresses are supported. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0.
Trap Port[1]	The port number on which the trap is sent. The default is 162.
Trap Severity	Specifies a severity level to assign to the trap. Open the pull-down menu and choose a level. The **Trap 1 Enabled** check box on the Network Properties dialog must be enabled to access this pull-down menu. Trap severity levels include Unknown, Emergency, Alert, Critical, Error, Warning, Notify, Info, Debug, and Mark

[1]Trap address (other than 0.0.0.0) and trap port combinations must be unique. For example, if trap 1 and trap 2 have the same address, then they must have different port values. Similarly, if trap 1 and 2 have the same port value, they must have different addresses.

4.10.3.4
Remote Logging

The Remote Logging (syslog) feature enables saving of the log information to a remote host that supports the syslog protocol. When enabled, the log entries are sent to the syslog host at the IP address that you specify in the Logging Host IP Address field. Log entries are saved in the internal switch log whether this feature is enabled or not.

To save log information to a remote host, you must edit the syslog.conf file (located on the remote host) and then restart the syslog daemon. Consult your operating system documentation for information on how to configure Remote Logging. The syslog.conf file on the remote host must contain an entry that specifies the name of the log file in which to save error messages. Add the following line to the syslog.conf file. A <tab> separates the selector field (local0.info) and action field which contains the log file path name (/var/adm/messages/messages.name).

```
local0.info <tab> /var/adm/messages.name
```

4.11 Archiving a Switch

You can create an .XML archive file containing the configuration parameters. Basically any data received by SANbox Manager is archived. However, user authentication and passwords are available only through the command line interface, and are not received by SANbox Manager, and thus are not archived. Archived parameters include the following:

- Switch properties and statistics
- IP configuration
- SNMP configuration
- Port properties and statistics
- Alarm configuration
- Zoning configuration

This archive file can be used to restore the configuration on the same switch or on a replacement switch. You can also use the archive file as a template for configuring new switches to add to a fabric. Security settings and user account information are not archived. The archive can be used later to restore the switch. Refer to ”Restoring a Switch” on page 4-30 for more information.

To archive a switch, do the following:

1. Open the Switch menu in the faceplate display and select **Archive**.
2. In the Save dialog, enter a file name.
3. Click the **Save** button.

4.12 Restoring a Switch

Restoring a switch loads the archived switch configuration parameters to the switch. The switch configuration must be archived before it can be restored. The switch archive must be compatible with the switch to be restored; that is, you can restore a SANbox2-8c switch only with an archive from a SANbox2-8c switch. Refer to ”Archiving a Switch” on page 4-30 for more information.

WARNING!! The switch being restored should be physically disconnected from the fabric. Restoring a switch in a fabric can severely disrupt the fabric. After the restore process is complete, the switch can be reconnected to the fabric.

To restore a switch, do the following:

1. Log in to the fabric through the switch you want to restore. You cannot restore a switch over an ISL.

2. Open the Switch menu in the faceplate display and select **Restore** to display the Restore dialog shown in Figure 4-13. The Restore dialog offers a **Full Restore** and a **Selective Restore** tab.

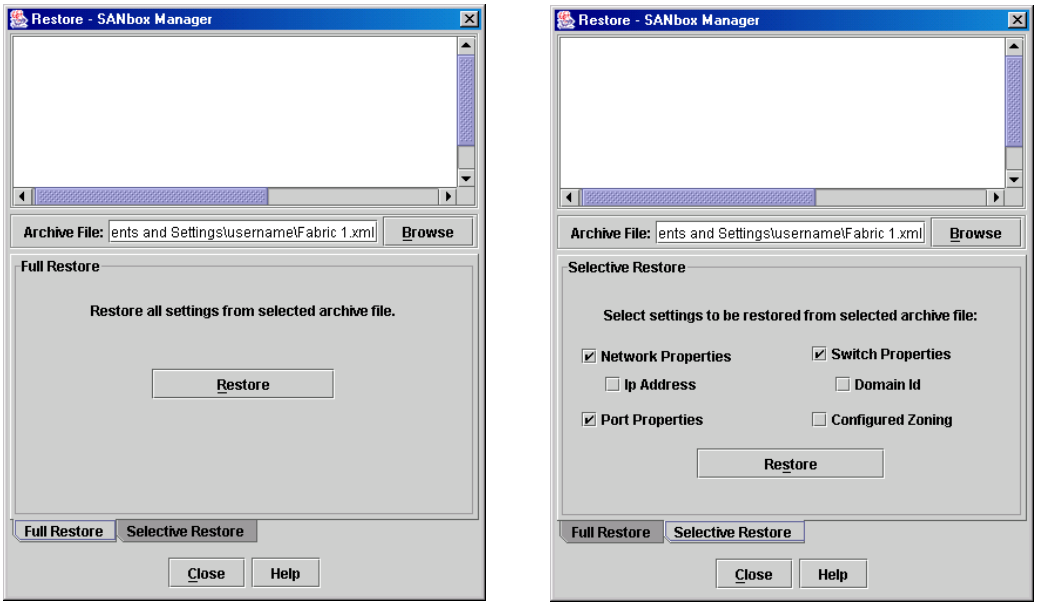


Figure 4-13. Restore Dialogs – Full and Selective

3. Enter the archive file name or browse for the file. This archive file must be one that was produced by the SANbox Manager Archive function. Configuration backup files created with the Config Backup command are not compatible with the SANbox Manager Restore function.
4. To restore all configuration settings, click the **Full Restore** tab, then click the **Restore** button. To restore selected configuration settings, click the **Selective Restore** tab and check one or more of the following boxes, then click the **Restore** button:
   - **Network Properties**: Restores all settings presented in the Network properties dialog except the IP address. Refer to ”Network Properties” on page 4-26.
   - **IP Address**: Restores switch IP address in addition to the other network properties.
   - **Switch Properties**: Restores all settings presented in the Switch properties dialog except the domain ID. Refer to ”Switch Properties” on page 4-21.
   - **Domain ID**: Restores switch domain ID in addition to the other switch properties.

- **Port Properties**: Restores all settings presented in the Port properties dialog. Refer to ”Configuring Ports” on page 5-10.
- **Configured Zoning**: Restores all zone sets, zones, and aliases in the switch’s zoning database.

4.13 Restoring the Factory Default Configuration

You can restore the switch and port configuration settings to the factory default values. To restore the factory configuration on a switch, open the Switch menu and select **Restore Factory Defaults**. Table 4-11 lists the factory default switch configuration settings.

Restoring the switch to the factory default configuration does not restore the account name and password settings. To restore user accounts, you must select the **Reset Password File** option in the maintenance menu. Refer to “Recovering a Switch” in the Installation Guide for your switch for information about maintenance mode and the maintenance menu.

Table 4-11. Factory Default Configuration Settings

Setting	Value
Symbolic name	SANbox2
Administrative state	Online
Domain ID	1
Domain ID Lock	False
In-band Management	True
Broadcast Support	Enable
Resource Allocation Timeout (RA TOV)	10000 milliseconds
FC-SW-2 Compliant	True
I/O Stream Guard	Disabled
Device Scan Enabled	True
Interop Credits	0
Error Detect Timeout (ED TOV)	2000 milliseconds
SNMP Enabled	True
SNMP Proxy	True
IP address	10.0.0.1
FDMI Enabled	True

Table 4-11. Factory Default Configuration Settings (Continued)

Setting	Value
FDMI HBA Entry Level	1000
Subnet mask address	255.0.0.0
Gateway address	10.0.0.254
Network Discovery	Static
Remote Logging	False
Remote Logging host IP address	10.0.0.254
Contact	Undefined
Location	Undefined
Trap enabled	False
Trap Port	162
Trap Address	Trap 1: 10.0.0.254; Traps 2-5: 0.0.0.0
Trap Community	Public
Read Community	Public
Write community	Private
Port State	Online
Port Speed	Auto-detect
Port Type	GL

4.14 Managing Firmware

The switch memory is partitioned for two firmware images. One of these partitions contains the active firmware; that is, the firmware version that is in use. The other partition contains the inactive firmware which is not in use. The pending firmware is the firmware that will be activated at the next switch reset. The pending firmware can be the active firmware or the inactive firmware. When you install new firmware, that image becomes the inactive firmware and the pending firmware. Upon resetting the switch, this image becomes both the active and pending firmware.

Firmware management tools enable you to do the following:

- Install and activate new firmware.
- Activate the pending firmware.
- Change the pending firmware.

Note: To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

4.14.1 Installing Firmware

Installing firmware involves loading, unpacking, and activating the firmware image on the switch. SANbox Manager does this in one operation. During a hotreset operation, fabric services will be unavailable for a short period (30-75 seconds depending on switch model). To ensure that an NDCLA operation is successful, verify that all administrative changes to the fabric (if any) are complete. When you need to do NDCLA/hotreset to multiple switches, only perform the NDCLA/hotreset on one switch at a time, and allow a 75 second wait before performing the NDCLA/hotreset operation on the next switch.

CAUTION! Changes to the fabric may disrupt the NDCLA process.

Common administrative operations that change the fabric include:

- Zoning modifications
- Adding, moving or removing devices attached to the switch fabric. This includes powering up or powering down attached devices.
- Adding, moving or removing ISLs or other connections.

Management Interfaces:

After an NDCLA operation is complete, management connections must be re-initiated:

- SANbox Manager sessions will re-connect automatically
- Telnet sessions must be restarted manually.

Applicable Code Versions:

- Future switch code releases will be upgraded non-disruptively unless specifically indicated in its associated release notes
- An NDCLA operation to previous switch code releases is not supported.

To install firmware, do the following:

1. In the faceplate display, open the Switch menu and select **Load Firmware**.
2. In the Firmware Upload dialog, click the **Select** button to browse and select the firmware file to be uploaded.
3. Click the **Start** button to begin the firmware load process.
4. SANbox Manager prompts you to activate the new firmware using a hot (non-disruptive) reset, if possible. Click the **OK** button to reset the switch and activate the new firmware.

4.14.2
Activating the Pending Firmware

To activate firmware that is both inactive and pending, open the Switch menu in the faceplate display and select **Activate Firmware**. SANbox Manager attempts a non-disruptive activation.

4.14.3
Changing the Pending Firmware

To change the pending firmware to the alternate image, do the following:

1. In the faceplate display, open the Switch menu and select **Firmware Fallback**.
2. The Firmware Fallback dialog prompts you to confirm the firmware version that is to become the pending firmware. Click the **Yes** button to select the fallback firmware or **No** to cancel.
3. SANbox Manager attempts a non-disruptive activation.

4.14.4
Displaying Hardware Status

A switch is equipped with the following chassis LEDs that provide hardware status information:

- Chassis Over Temperature LED - indicates the temperature status of the switch.
- Fan Fail LED - indicates operational status of both fans.
- Heartbeat LED - indicates the status of the internal switch processor and the results of the power-on self test (POST).
- Input Power LED - indicates the voltage status of the switch.

In the SANbox2-8c and SANbox2-16 faceplate displays, you can display a summary of this status information by placing the cursor on the chassis LED cluster as shown in Figure 4-14. Refer to the installation guide for your switch for more information about the chassis LEDs.

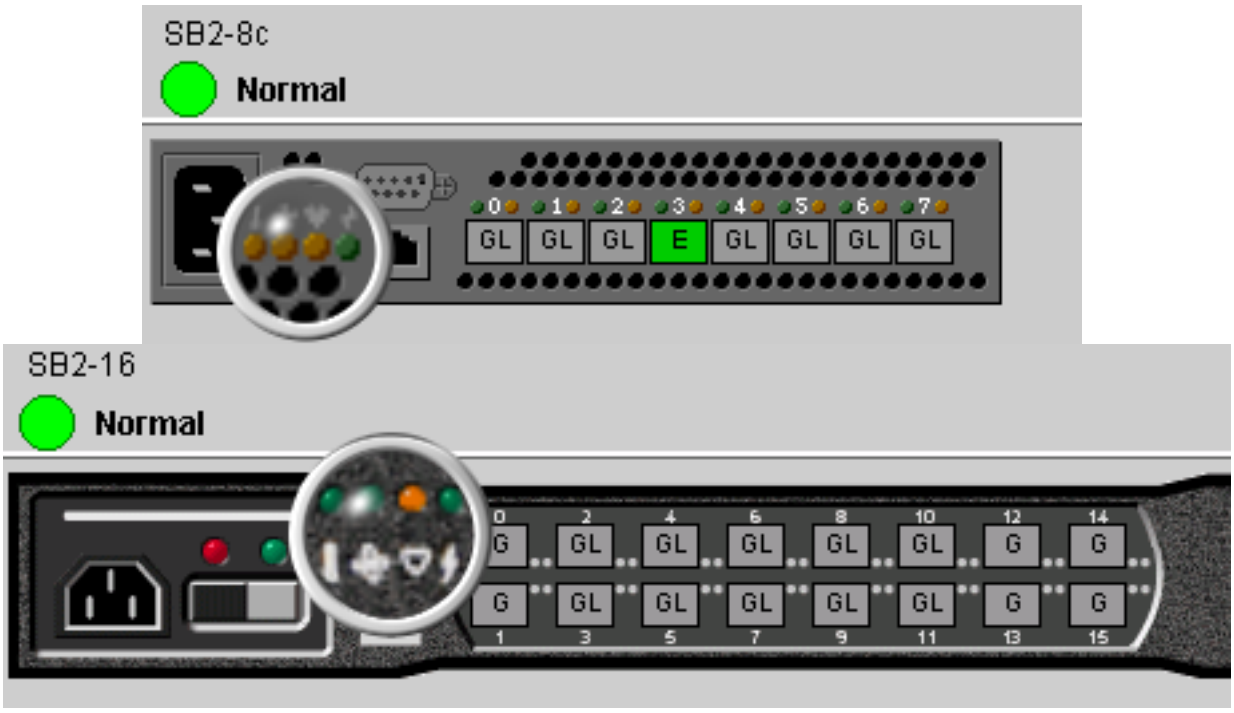


Figure 4-14. Hardware Status LEDs

Section 5

Managing Ports

This section describes the following tasks that manage ports and devices:

- Displaying port information
- Configuring ports
- Testing ports

5.1 Displaying Port Information

Port information is available primarily in the faceplate display shown in Figure 5-1. The faceplate display data windows provide information and statistics for switches and ports. Use the topology display to view status information on fabrics, switches, and links between switches.

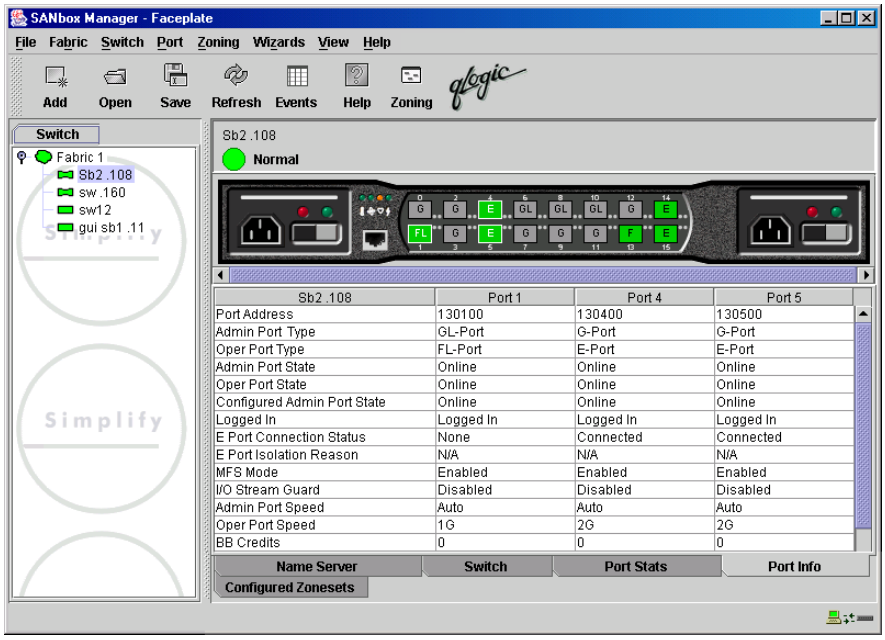

SANbox Manager - Faceplate
File Fabric Switch Port Zoning Wizards View Help
Add Open Save Refresh Events Help Zoning
Switch
Fabric 1
Sb2 .108
sw .160
sw12
gui sb1 .11
Sb2 .108
Normal
Sb2 .108 | Port 1 | Port 4 | Port 5
Port Address | 130100 | 130400 | 130500
Admin Port Type | GL-Port | G-Port | G-Port
Oper Port Type | FL-Port | E-Port | E-Port
Admin Port State | Online | Online | Online
Oper Port State | Online | Online | Online
Configured Admin Port State | Online | Online | Online
Logged In | Logged In | Logged In | Logged In
E Port Connection Status | None | Connected | Connected
E Port Isolation Reason | N/A | N/A | N/A
MFS Mode | Enabled | Enabled | Enabled
I/O Stream Guard | Disabled | Disabled | Disabled
Admin Port Speed | Auto | Auto | Auto
Oper Port Speed | 1G | 2G | 2G
BB Credits | 0 | 0 | 0
Name Server
Switch
Port Stats
Port Info
Configured Zonesets

Figure 5-1. Faceplate Display – Port Information

5.1.1
Monitoring Port Status

The faceplate display provides the following port related information:

- Port type
- Port operational state
- Port speed
- Port media

To display port number and status information for a port, position the cursor over a port on the faceplate display. The status information changes depending on the View menu option selected.

5.1.1.1
Displaying Port Types

To display port type status, from the faceplate display, open the View menu, and select **View Port Types**. Table 5-1 lists the possible port types and their meanings.

Table 5-1. Port Types

Type	Description
F_Port	Fabric port - Supports a single public device (N_Port).
FL_Port	Fabric loop port - Self discovers a single device (N_Port) or a loop of up to 126 public devices (NL_Port).
G_Port	Generic port - Self discovers as an F_Port or an E_Port.
GL_Port	Generic loop port - Self discovers as an F_Port, FL_Port, or an E_Port. GL_Port is the default port type. A single device on a public loop will attempt to configure as an F_Port first, then if that fails, as an FL_Port.
Donor	Donor port - Allows buffer credits to be used by another port.

5.1.1.2

Displaying Port Operational States

To display the operational state on each port in the faceplate display, open the View menu and select **View Port States**. Table 5-2 lists the possible operational states and their meanings. The port operational state refers to actual port state and not the administrative state you may have assigned.

Table 5-2. Port Operational States

State	Description
On	Online – port is active and ready to send data.
Ia	Inactive – port operational state is offline, but administrative state is online.
Iso	Isolated – E_Port has lost its connection. Refer to ”Port Information Data Window” on page 5-7 for information about why the E_Port has isolated.
Off	Offline – port is active, can receive signal, but cannot accept a device login.
Dia	Diagnostics – port is in diagnostics mode in preparation for testing
Dn	Down – the port is disabled, power is removed from the lasers, and can’t be logged in.

5.1.1.3

Displaying Port Speeds

To display the speed of each port in the faceplate display, open the View menu and select **View Port Speeds**. Table 5-3 lists the possible port speeds.

Table 5-3. Port Speeds

Speed	Description
Au	Auto-detect
1Gb	1 Gbps transmission speed
2Gb	2 Gbps transmission speed

5.1.1.4
Displaying Transceiver Media Status

To display transceiver media status, open the View menu and select **View Port Media**. Table 5-2 lists the port media states and their meanings.

Table 5-4. Transceiver Media View

Media Icon	Description
	Optical SFP (Green), logged-in, active, and ready to send data.
	Optical SFP (Gray), not logged-in, active, can receive signal, but cannot accept a device login
	Copper SFP, (Copper)
None	Empty port, no transceiver installed

5.1.2
Port Statistics Data Window

The Port Statistics data window displays statistics about port performance. To open the Port Statistics window, select one or more ports in the faceplate display and click the **Port Stats** tab below the data window. Table 5-5 describes the Port Statistics data window entries.

The Statistics pull-down menu is available on the Port Statistics data window, and provides different ways to view detailed port information. Click the down arrow to open the pull-down menu. Open the pull-down menu and select **Absolute** to view the total count of statistics since the last switch or port reset. Select **Rate** to view the number of statistics counted per second over the polling period. Select **Baseline** to view the total count of statistics since the last time the baseline was set. When viewing baseline statistics, click the **Clear Baseline** button to set the current baseline. The baseline will also be set when the switch status changes from unreachable to reachable.

Table 5-5. Port Statistics Data Window Entries

Entry	Description
Start Time	The beginning of the period over which the statistics apply. The start time for the Absolute view is not applicable. The start time for the Rate view is the beginning of polling interval. The start time for the Baseline view is the last time the baseline was set.
End Time	The last time the statistics were updated on the display.
Total Time	Total time period from start time to end time.
Al Init	Number of times the port entered the initialization state.
AL Init Error	Number of times the port entered initialization and the initialization failed. Increments count when port has a sync loss.
Bad Frames	Number of frames that were truncated due to a loss of sync or the frame didn't end with an EOF.
Class 2 Frames In	Number of class 2 frames received by this port.
Class 2 Frames Out	Number of class 2 frames transmitted by this port.
Class 2 Words In	Number of class 2 words received by this port.
Class 2 Words Out	Number of class 2 words transmitted by this port.
Class 3 Frames In	Number of class 3 frames received by this port.
Class 3 Frames Out	Number of class 3 frames transmitted by this port.
Class 3 Toss	Number of class 2 and class 3 sequences that were discarded by this port. A sequence can be discarded because of detection of a missing frame (based on SEQ_CNT), detection of an E_D_TOV timeout, receiving a reject frame, receiving frames for a stopped sequence, or other causes.
Class 3 Words In	Number of class 3 words received by this port.
Class 3 Words Out	Number of class 3 words transmitted by this port.
Decode Errors	Number of invalid transmission words detected during decoding. Decoding is from the 10-bit characters and special K characters.
Ep Connects	Number of E_Port logins.
FBusy	Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_port that is preventing delivery of this frame.

Table 5-5. Port Statistics Data Window Entries (Continued)

Entry	Description
Flow Errors	Number of times a frame is received and all the switch ports receive buffers are full. The normal Fabric Login exchange of flow control credit should prevent this from occurring. The frame will be discarded.
FReject	Number of frames, from devices, that have been rejected. Frames can be rejected for any of a large number of reasons.
Invalid CRC	Number of invalid Cyclic Redundancy Check (CRC) frames detected.
Invalid Destination Address	Number of address identifier (S_ID, D_ID) errors. AL_PA equals non-zero AL_PA found on F_Port.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or by loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
LIP (AL_PD,AL_PS)	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.
LIP(f7,AL_PS)	This LIP is used to reinitialize the loop. An L_port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.
LIP(f7,f7)	A loop initialization primitive frame used to acquire an AL_PA.
LIP(f8,AL_PS)	This LIP denotes a loop failure detected by the L_port identified by AL_PS.
Login Count	Number of device logins that have occurred on the switch.
Logout Count	Number of device logouts that have occurred on the switch.
Loop Timeouts	Number of loop timeouts.
Loss Of Sync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
Primitive Sequence Errors	Number of bad primitives received by the port.
Rx Link Resets	Number of link reset primitives received from an attached device.
Rx Offline Sequences	Number of offline sequence primitives received by the port.

Table 5-5. Port Statistics Data Window Entries (Continued)

Entry	Description
Total Errors	Total number of primitive and non-primitive port link errors.
Total Link Resets	Number of link-reset primitives the transmitted by the port.
Total LIPs Received	Number of loop initialization primitive frames received.
Total LIPs Transmitted	Number of loop initialization primitive frames transmitted.
Tx Offline Sequences	Number of offline primitives transmitted by the port.
Total Rx Frames	Total number of frames received by the port.
Total Rx Words	Total number of words received by the port.
Total Tx Frames	Total number of frames transmitted by the port.
Total Tx Words	Total number of words transmitted by the port.
Tx Link Resets	Number of link reset primitives sent from this port to an attached port.
Total Offline Sequences	Total number of offline sequences transmitted and received by the port.

5.1.3 Port Information Data Window

The Port Information data window displays port detail information for the selected port. To open the Port Information data window, click the **Port Info** tab below the data window in the faceplate display.

Table 5-6. Port Information Data Window Entries

Entry	Description
Port Address	Port Fibre Channel address.
Administrative Port Type	The port type (G, GL, F, FL, or Donor) that the port is configured as. This value is persistent; it will be maintained during a switch reset. During port an auto-configuration it will be used to determine which operational port states are allowed.
Operational Port Type	The port type that is currently active. This will be set during port auto-configuration based on the administrative port type.

Table 5-6. Port Information Data Window Entries (Continued)

Entry	Description
Administrative Port State	The port state (Online, Offline, Diagnostics, or Down) which has been set by the user. This state may be different from the configured administrative state if the user has not saved it in the switch configuration. This state is used at the time it is set to try to set the port operational state. This value is not persistent and will be lost on a switch reset.
Operational Port State	The port state that is currently active. This value may be different from the administrative port state, for example due to an error condition.
Configured Administrative Port State	The port state (Online, Offline, Diagnostics, or Down) which is saved in the switch configuration, either by the user or at the factory. This value is persistent; it will be maintained during a switch reset, and will be used after a reset to set the port operational state.
Logged In	Indicates whether logged in or not.
E Port Connection Status	Whether or not the E_Port is currently active. It can hold the values None, Connecting, Connected or Isolated.
E Port Isolation Reason	Why E_Port is isolated.
MFS Mode	Port tuning indicator.
I/O Stream Guard	Whether RSCN suppression is enabled or disabled.
Administrative Port Speed	The speed requested by the user.
Operational Port Speed	The speed actually being used by the port.
Interop Credits	Whether Interop credits have been set.
Device Scan	Queries the connected device during login for FC-4 descriptor information. Disable this parameter only if the scan creates a conflict with the connected device.
Symbolic Name	Port symbolic name

Table 5-6. Port Information Data Window Entries (Continued)

Entry	Description
Ext Credits Requested	Whether extended credits have been requested for ports.
Credits to Donate	The number of credits available to be donated by the selected port.
Donor Group	The donor group of the selected port.
Valid Donor Groups	The number of separate groups within which extended credits may be donated and assigned.
Medium	The transceiver type.

5.1.4 Name Server Data Window

The Name Server data window displays information about devices (hosts and storage targets) connected to the switch. To open the Name Server data window from the topology or faceplate display, click the **Name Server** tab below the data window. In the topology display, if no switches are selected, the name-server entries for the entire fabric are displayed in the data window; if switches are selected, then only the devices attached to the selected switches are displayed. In the faceplate display, only the devices attached the switch being viewed are displayed. Refer to Table 4-2 for a description of the Name Server data window entries.

5.2 Configuring Ports

The port settings or characteristics are configured using the Port Properties dialog shown in Figure 5-2. To open the Port Properties dialog, select one or more ports, open the Port menu and select **Port Properties**.

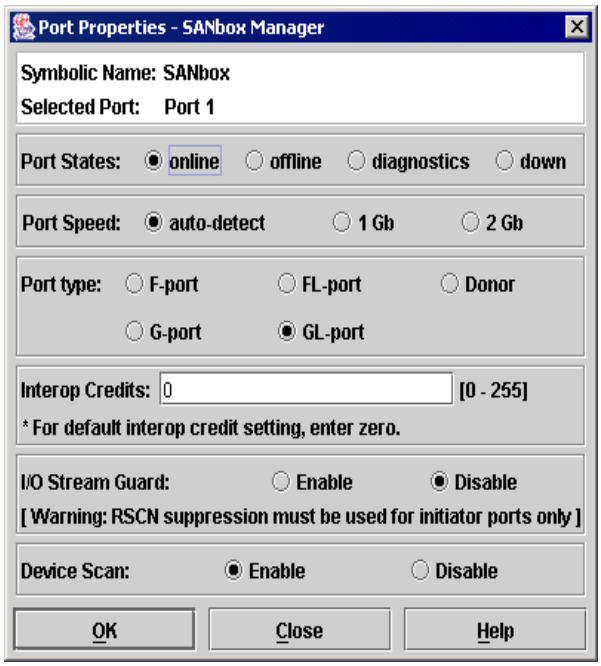

Port Properties - SANbox Manager
Symbolic Name: SANbox
Selected Port: Port 1
Port States: online offline diagnostics down
Port Speed: auto-detect 1 Gb 2 Gb
Port type: F-port FL-port Donor
G-port GL-port
Interop Credits: 0 [0 - 255]
* For default interop credit setting, enter zero.
I/O Stream Guard: Enable Disable
[Warning: RSCN suppression must be used for initiator ports only]
Device Scan: Enable Disable
OK
Close
Help

Figure 5-2. Port Properties Dialog

The Port Properties dialog displays the switch name and the selected port(s). Use the Port Properties dialog to change the following parameters:

- Port state
- Port speed
- Port type
- Interoperability credits
- Port symbolic name
- I/O Stream Guard (RSCN Suppression)
- Device scan
- Extending port credits

5.2.1
Changing Port Administrative States

The port administrative state determines the operational state of a port. The port administrative state exists in two forms: the configured administrative state and the current administrative state.

- The configured administrative state is the state that is saved in the switch configuration and is preserved across switch resets. SANbox Manager always makes changes to the configured administrative state.
- The current administrative state is the state that is applied to the port for temporary purposes and is not preserved across switch resets. The current administrative state is set using the Set Port command. Refer to the "Set Port Command" on page A-46.

Table 5-7 describes the port administrative states. To change port administrative state, do the following:

1. Select one or more ports in the faceplate display.
2. Open the Port menu and select **Port Properties** to open the Port Properties dialog.
3. Click the **Port States** radio button that corresponds to the port state you want.
4. Click the **OK** button to write the new port state to the switch.

Table 5-7. Port Administrative States

State	Description
Online	Activates and prepares port to send data.
Offline	Prevents port from receiving signal and accepting a device login.
Diagnostics	Prepares port for testing and prevents the port from accepting a device login.
Down	Disables the port.

5.2.2
Changing Port Speeds

Ports are capable of transmitting and receiving at 1 or 2 Gbps. The ports can be configured for either transmission speed or to sense the transmission speed of the device to which it is connected. Table 5-8 describes the port speeds. To change the port speed, do the following:

1. Select one or more ports in the faceplate display.
2. Open the Port menu and select **Port Properties**.
3. Click the radio button that corresponds to the port speed you want.
4. Click the **OK** button to write the new port speed to the switch.

Table 5-8. Port Speeds

State	Description
Auto-Detect	Matches the transmission speed of the connected device. This is the default.
1Gb	Sets the transmission speed to 1 Gbps.
2Gb	Sets the transmission speed to 2 Gbps.

5.2.3
Changing Port Types

The ports can be configured to self-discover the proper type to match the device or switch to which it is connected. Table 5-9 describes the port types. To change the port type, do the following:

1. Select one or more ports in the faceplate display.
2. Open the Port menu and select **Port Properties** to open the Port Properties dialog.
3. Click the **Port Type** radio button for the port type you want.
4. Click the **OK** button to write the new port type to the switch.

Table 5-9. Port Types

State	Description
F_Port	Fabric port - Supports a single public device (N_Port).
FL_Port	Fabric loop port - Self discovers a single device (N_Port) or a loop of up to 126 public devices (NL_Port).
G_Port	Generic port - Self discovers as an F_Port or an E_Port.

Table 5-9. Port Types (Continued)

State	Description
GL_Port	Generic loop port - Self discovers as an F_Port, FL_Port, or an E_Port. GL_Port is the default port type. A single device on a public loop will attempt to configure as an F_Port first, then if that fails, as an FL_Port.
Donor	Donor port - Allows buffer credits to be used by another port.

5.2.4
Changing Interoperability Credits

SANbox2 switches negotiate with other switches to resolve differences in the number of port buffer credits. However, certain non-FC-SW-2-compliant switches do not negotiate and will isolate when connected. To remedy this situation, disconnect the switches, then reconfigure the SANbox2 E_Port to match the number of port buffer credits on the other switch.

Note: Changing interop credits is necessary only for E_Ports that are connected to non-FC-SW-2-compliant switches. Contact your authorized maintenance provider for assistance in using this feature.

To change interoperability credits to permit operation with non-compliant switches, do the following:

1. Determine the number of credits per port for the non-compliant switch:
   - If the credits per port is equal to 16, stop here – no changes are needed.
   - If the credits per port is less than 16, proceed to step 2.
   - If the credits per port is greater than 16, you must extend credits for the affected SANbox2 port to increase the number of credits to match that of the non-standard switch. Refer to ”Extending Port Credits” on page 5-14.
2. Select the SANbox2 switch ports in the faceplate display that are to serve as links to the non-compliant switch.
3. Open the Port menu and select **Port Properties**.
4. In the **Interop Credits** field, enter the number of credits per port of the non-compliant switch and click the **OK** button.
5. Connect the switches.

5.2.5
Changing Port Symbolic Name

To change the symbolic name of a port from the faceplate display, do the following:

1. Open the faceplate display and select a port.
2. Open the Port menu and select **Port Symbolic Name**.
3. In the Port Symbolic Name dialog, choose one of the following:
   - Enter a new name for the port in the Set Port Symbolic Name field.
   - Check the **Restore Default Port Symbolic** Name check box to restore the default name.
4. Click the **OK** button.

5.2.6
I/O Stream Guard

The I/O Stream Guard feature suppresses the generation of Registered State Change Notification (RSCN) messages on a port basis. I/O Stream Guard should be enabled only on ports connected to initiator devices. To suppress the generation of RSCN messages for the selected port, open the Port menu, and click **Enable** radio button in the I/O Stream Guard area of the Port Properties dialog.

5.2.7
Scan Device

The Device Scan feature queries the connected device during login for FC-4 descriptor information. Disable this parameter only if the scan creates a conflict with the connected device.

5.2.8
Extending Port Credits

Each port is supported by a data buffer with a 16 credit capacity; that is, 16 maximum sized frames. For fiber optic cables, this enables full bandwidth service over a distance of 26 kilometers at 1 Gbps (0.6 credits/Km), or 13 kilometers at 2 Gbps (1.2 credits/Km). Longer distances can be spanned at full bandwidth by borrowing credits from designated donor ports thus pooling the buffer capacities. This is called *credit extension*. Each donor port contributes 15 credits to the pool from which the recipient ports can draw. For example, one donor port contributes 15 credits to the pool from which a recipient draws for a total of 31 credits (15+16). This provides approximately 52 Km at 1 Gbps (31÷0.6) or 26 Km at 2 Gbps (31÷1.2).

To extend credits, open the Wizards menu and select **Ext Credit Wizard**. The Extended Credit Wizard leads you through the following process to extend credits based on transmission distance requirements:

1. Extended Distance on SANbox2: Explains the concepts and principles of extending port credits. Click the **Next** button.
2. Extended Distance Requirements: Specify speed and distance requirements for each port then click the **Next** button.
3. Designate Donor Ports: Select available ports and click **>>** to move the port into the Selected Donor Port column shown in Figure 5-3. Match the number of ports needed with the number of designated donor ports. Click the **Next** button.

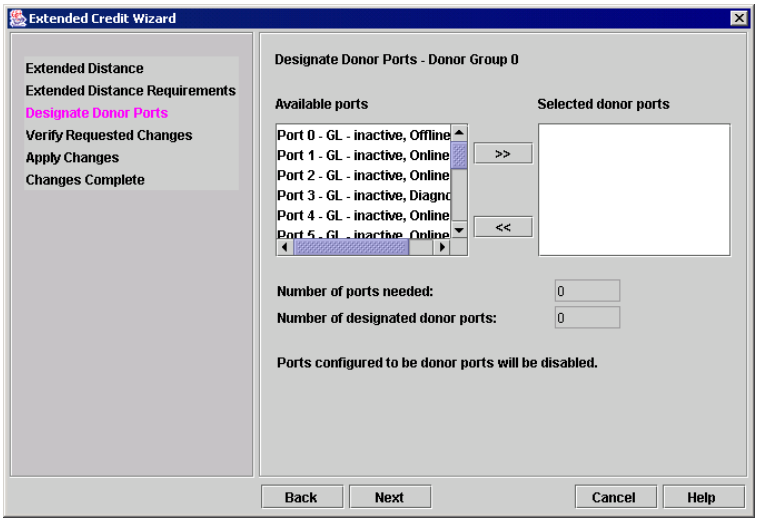


Figure 5-3. Designate Donor Ports

4. Verify Requested Changes: Review the extended distance requests and the selected donor ports. Click the **Finish** button to apply the changes, and redistribute the credits.

Note: As credits are used, the Logged-In LEDs on the corresponding donor ports illuminate continuously. In addition, donor port Activity LEDs will reflect the same traffic as the recipient port. Donor ports whose credits are being used are unavailable to devices that are connected to them.

5.3 Resetting a Port

The Reset Port option reinitializes the port using the saved configuration. To reset a port, do the following:

1. In the faceplate display, select the ports to be reset.
2. Open the Port menu and select **Reset Port**.

5.4 Testing Ports

The port loopback tests verify correct port operation by sending a frame out through the loop, and then verifying that the frame received matches the frame that was sent. Only one port can be tested at a time for each type of test. The Port Loopback Test dialog shown in Figure 5-4 presents the following loopback tests:

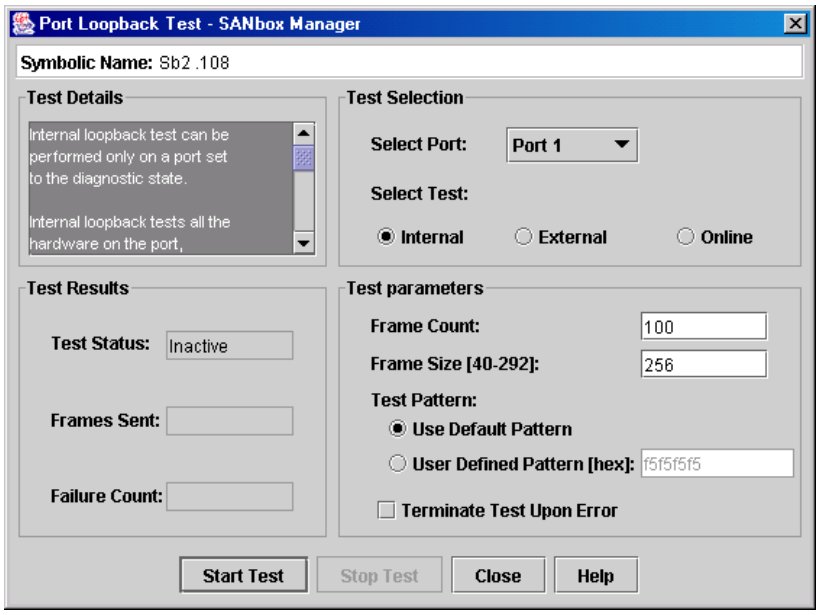


Figure 5-4. Port Loopback Test Dialog

- **SerDes level (Internal)** - The SerDes level test verifies port circuitry. The SerDes level test sends a test frame from the ASIC through the SerDes chip and back to the ASIC for the selected ports. The port passes the test if the frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and therefore, disrupts communication.
- **SFP level (External)** - The SFP level test verifies port circuitry. The SFP level test sends a test frame from the ASIC through the SerDes chip, through the SFP transceiver fitted with an external loopback plug, and back

to the ASIC for the selected ports. The port passes the test if the test frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and therefore, disrupts communication.

- **Node-to-Node (Online)** - The Node-to-Node test verifies communications between the port and its device node or device loop. The port being tested must be online and connected to a remote device. The port passes the test if the frame that was sent by the ASIC matches the frame that was received. This test does not disrupt communication on the selected port. This test requires that the port be online, and therefore, does not disrupt communication.

To run the internal, external, or online port loopback test on a port, do the following:

1. In the faceplate display, select the port to be tested.
2. Open the Port menu and select **Port Loopback Test** to open the Port Loopback Test dialog.
3. In the Test Selection area, click the radio button for the type of loopback test to be run (Internal, External, or Online). If you choose the internal or external test, SANbox Manager will prompt you to confirm that the port state needs to be changed to the diagnostic state. Click the **OK** button and SANbox Manager will change the port state.
4. Enter the frame count, frame size, and click a test pattern radio button. You may use the default pattern or enter an 8-digit pattern (hex). For online test, you can check the **Terminate Test Upon Error** check box if you want the test to stop should it encounter an error.
5. Click the **Start Test** button to begin the test. The Test Results area displays the test status, number of frames sent, and number of errors found.
6. To test another port, open the Select Port pull-down menu and select another port (number) and test type (Internal, External, or Online) in the Test Selection area.
7. Click the **Start Test** button to begin the next test. Observe the results in the Test Results area.

Notes

Appendix A
Command Line Interface

The command line interface (CLI) enables you to perform a variety of fabric and switch management tasks through an Ethernet or a serial port connection. This section describes the following:

- Logging on to a switch
- User accounts
- Working with switch configurations
- Commands

A.1 Logging On to a Switch

To log on to a switch using Telnet, open a command line window on the workstation and enter the Telnet command followed by the switch IP address:

```
# telnet ip_address
```

A Telnet window opens prompting you for a login. Enter an account name and password.

To log on to a switch through the serial port, configure the workstation port with the following settings:

- 9600 baud
- 8-bit character
- 1 stop bit
- No parity

Enter an account name and password when prompted.

A.2 User Accounts

Switches come from the factory with the following user account already defined:

Account name: admin
Password: password
Authority: Admin

This user account provides full access to the switch and its configuration. After planning your fabric management needs and creating your own user accounts, consider changing the password for this account. Refer to ”Commands” on page A-5 for more information about authority levels. Refer to the ”User Command” on page A-80 for information about creating user accounts.

Note: A switch supports a combined maximum of 19 logins or sessions reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 15 logins or sessions for SANbox Manager in-band and out-of-band logins, Application Programming Interface (API) in-band and out-of-band logins, and Telnet logins. Of these 15, there can be a combined maximum of 6 SANbox Manager and API logins. Additional logins will be refused. Each added fabric will consume a session on all managed switches in the fabric.

A.3 Working with Switch Configurations

Successful management of switches and fabrics with the command line interface depends on the effective use of switch configurations. Modifying configurations, backing up configurations, and restoring configurations are key switch management tasks.

A.3.1 Modifying a Configuration

A switch supports up to 10 configurations including the default configuration. Each switch configuration contains switch, port, port threshold alarm, and zoning configuration components.

The Show Switch command displays the name of the active configuration. A configuration name can have up to 31 characters excluding the pound symbol (#), semicolon (;), and comma (,). By editing the latest configuration and saving the results under a new name, you can create a history of configuration changes. Use the Config List command to display the names of the configurations stored on the switch

```
SANbox2 #> config list
  Current list of configurations
  ------------------------------
  default
  config_10132003
```

To modify a switch configuration you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time either through Telnet or SANbox Manager. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name the active configuration is assumed. The Config Edit session provides access to the

Set Config commands with which you make modifications to the port, switch, port threshold alarm, or zoning configuration components as shown:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit default
   The config named default is being edited.
SANbox2 (admin-config)#> set config port . . .
SANbox2 (admin-config)#> set config switch . . .
SANbox2 (admin-config)#> set config threshold . . .
SANbox2 (admin-config)#> set config zoning . . .
```

The Config Save command saves the changes you made during the Config Edit session. In this case, changes to the configuration named *Default* are being saved to a new configuration named *config_10132003*. However, the new configuration does not take effect until you activate it with the Config Activate command as shown:

```
SANbox2 (admin-config)#> config save config_10132003
SANbox2 (admin-config)#> config activate config_10132003
SANbox2 (admin-config)#> admin end
SANbox2 #>
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

A.3.2
Backing up and Restoring Switch Configurations

Backing up and restoring a configuration is useful to protect your work or for use as a template in configuring other switches. The Config Backup command creates a file on the switch, named *configdata*. This file can be used to restore a switch only with the command line interface; it cannot be used to restore a switch using SANbox Manager.

```
SANbox2  #> admin start
SANbox2 (admin) #> config backup
```

The *configdata* file contains all of the switch configuration information including the following:

- All named switch configurations including the default configuration. This includes port, switch, port threshold alarm, and zoning configuration components.
- All SNMP and network information defined with the Set Setup command.
- The zoning database included all zone sets, zones, and aliases

You use FTP to download the *configdata* file to your workstation for safe keeping and to upload the file back to the switch for the restore function. To download the configdata file, open an FTP session on the switch and login with the account name *images* and password *images*. Transfer the file in binary mode with the Get command as shown:

```
>ftp ip_address
user:images
password: images

ftp>bin
ftp>get configdata
    xxxxx bytes sent in xx secs.
ftp>quit
```

You should rename the *configdata* file on your workstation with the switch name and date, *config_switch_169_10112003*, for example.

The restore operation begins with FTP to upload the configuration file from the workstation to the switch, then finishes with a Telnet session and the Config Restore command. To upload the configuration file, *config_switch_169_10112003* in this case, open and FTP session with account name *images* and password *images*. Transfer the file in binary mode with the Put command as shown:

```
ftp ip_address
user:images
password: images
ftp> bin
ftp> put
  Local file config_switch_169_10112003
  Remote file configdata
    ftp>quit
```

The restore process replaces all configuration information on the switch and afterwards the switch is automatically reset. If the restore process changes the IP address, all management sessions are terminated. Use the Set Setup System command to return the IP configuration to the values you want. Refer to the ”Set Setup Command” on page A-48. To restore the switch, open a Telnet session, then enter the Config Restore command from within an Admin session as shown:

```
SANbox2  #> admin start
SANbox2 (admin) #> config restore
  The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
```

A.4 Commands

The command syntax is as follows:

command
keyword
keyword *[value]*
keyword [value1] [value2]

The **Command** is followed by one or more keywords. Consider the following rules and conventions:

- Commands and keywords are case insensitive.
- Required keyword values appear in standard font: [value]. Optional values are shown in italics: *[value].*
- Underlined portions of the keyword in the command format indicate the abbreviated form that can be used. For example the Delete keyword can be abbreviated Del.

The command-line completion feature makes entering and repeating commands easier. Table A-1 describes the command-line completion keystrokes.

Table A-1. Command-Line Completion

Keystroke	Effect
Tab	Completes the command line. Enter at least one character and press the tab key to complete the command line. If more than one possibility exists, press the Tab key again to display all possibilities.
Up Arrow	Scrolls backward through the list of previously entered commands.
Down Arrow	Scrolls forward through the list of previously entered commands.
Control-A	Moves the cursor to the beginning of the command line
Control-E	Moves the cursor to the end of the command line.

The command set performs monitoring and configuration tasks. Commands related to monitoring tasks are available to all account names. Commands related to configuration tasks are available only within an admin session. An account must have Admin authority to enter the Admin Start command, which opens an admin session. Refer to the ”Admin Command” on page A-7.

The commands and their page numbers are listed in Table A-2.

Table A-2. Commands Listed by Authority Level

Monitoring Commands		Configuration Command	
Help	(A-16)	Admin	(A-7)
History	(A-17)	**Admin Session Commands**	
Ping	(A-22)		
Ps	(A-23)	Alias[1]	(A-8)
Quit	(A-24)	Config[1]	(A-10)
Show	(A-53)	Date[1]	(A-13)
Show Config	(A-65)	Fallback	(A-14)
Show Log	(A-68)	Hardreset	(A-15)
Show Perf	(A-71)	Hotreset	(A-18)
Show Setup	(A-73)	Image	(A-19)
Uptime	(A-79)	Lip	(A-20)
Whoami	(A-83)	Passwd	(A-21)
		Reset	(A-25)
		Set[1]	(A-30)
		Set Config	(A-32)
		Set Log	(A-43)
		Set Port[1]	(A-46)
		Set Setup	(A-48)
		Shutdown	(A-75)
		Test	(A-76)
		User[1] [2]	(A-80)
		Zone[1]	(A-84)
		Zoneset[1]	(A-88)
		Zoning[1]	(A-90)

[1]Some keywords do not require an Admin session.

[2] Some keywords can be executed only by the Admin account name.

Admin Command

Opens and closes an Admin session. The Admin session provides commands that change the fabric and switch configurations. Only one Admin session can be open on the switch at any time. An inactive Admin session will time out after a period of time which can be changed using the Set Setup System command. Refer to the ”Set Setup Command” on page A-48.

Authority Admin

Syntax **admin**
start (or begin)
end (or stop)
cancel

Keywords **start (or begin)**
Opens the admin session.

end (or stop)
Closes the admin session. The Hardreset, Hotreset, Logout, Shutdown, and Reset Switch commands will also end an admin session.

cancel
Terminates an Admin session opened by another user. Use this keyword with care because it terminates the Admin session without warning the other user and without saving pending changes.

Notes Closing a Telnet window during an admin session does not release the session. In this case, you must either wait for the admin session to time out, or use the Admin Cancel command.

Examples The following example shows how to open and close an Admin session:

```
SANbox2 #> admin start


SANbox2 (admin) #>


.
.
.


SANbox2 (admin) #> admin end
SANbox2 #>
```

Alias Command

Creates a named set of ports/devices. Aliases make it easier to assign a set of ports/devices to many zones. An alias can not have a zone or another alias as a member.

Authority Admin session for all keywords except List and Members

Syntax **alias**

add [alias] [member_list]
copy [alias_source] [alias_destination]
create [alias]
delete [alias]
list
members [alias]
remove [alias] [member_list]
rename [alias_old] [alias_new]

Keywords **add [alias] [member_list]**
Specifies one or more ports/devices given by [member_list] to add to the alias named [alias]. Use a <space> to delimit ports/devices in [member_list]. An alias can have a maximum of 2000 members. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.

The application verifies that the [alias] format is correct, but does not validate that such a port/device exists.

copy [alias_source] [alias_destination]
Creates a new alias named [alias_destination] and copies the membership into it from the alias given by [alias_source].

create [alias]
Creates an alias with the name given by [alias]. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 aliases.

delete [alias]
Deletes the specified alias given by [alias] from the zoning database. If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all aliases. This keyword does not require an admin session.

members [alias]
Displays all members of the alias given by [alias]. This keyword does not require an admin session.

remove [alias] [member_list]
Removes the ports/devices given by [member_list] from the alias given by [alias]. Use a <space> to delimit ports/devices in [member_list]. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) for the device with the format xx:xx:xx:xx:xx:xx:xx:xx.

rename [alias_old] [alias_new]
Renames the alias given by [alias_old] to the alias given by [alias_new].

Config Command

Manages the Fibre Channel configurations on a switch. For information about setting the port and switch configurations, refer to the ”Set Config Command” on page A-32.

Authority Admin session for all keywords except List

Syntax

config
activate *[config_name]*
backup
cancel
copy [config_source] [config_destination]
delete [config_name]
edit *[config_name]*
list
restore
save *[config_name]*

Keywords

activate *[config_name]*
Activates the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used. Only one configuration can be active at a time.

backup
Creates a file named *configdata*, which contains the system configuration information. To download this file, open an FTP session, log in with account name/password of “images” for both, and type “get configdata”. Refer to ”Backing up and Restoring Switch Configurations” on page A-3.

cancel
Terminates the current configuration edit session without saving changes that were made.

copy [config_source] [config_destination]
Copies the configuration given by [config_source] to the configuration given by [config_destination]. The switch supports up to 10 configurations including the default configuration.

delete [config_name]
Deletes the configuration given by [config_name] from the switch.

edit *[config_name]*
Opens an edit session for the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used.

list
Displays a list of all available configurations on the switch. This keyword does not require an admin session.

restore
Restores configuration settings to an out-of-band switch from a backup file named *configdata*, which must be first uploaded on the switch using FTP. You create the backup file using the Config Backup command. Use FTP to load the backup file on a switch, then enter the Config Restore command. After the restore is complete, the switch automatically resets. Refer to "Backing up and Restoring Switch Configurations" on page A-3.

Note:
- If the restore process changes the IP address, all management sessions are terminated. Use the Set Setup System command to return the IP configuration to the values you want. Refer to the "Set Setup Command" on page A-48.
- Configuration archive files created with the SANbox Manager Archive function are not compatible with the Config Restore command.

save *[config_name]*
Saves changes made during a configuration edit session in the configuration given by [config_name]. If you omit [config_name], the value for [config_name] you chose for the most recent Config Edit command is used. [config_name] can be up to 31 characters excluding #, semicolon (;), and comma (,). The switch supports up to 10 configurations including the default configuration.

Notes

If you edit the active configuration, changes will be held in suspense until you reactivate the configuration or activate another configuration.

Examples

The following shows an example of how to open and close a Config Edit session:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
   The config named default is being edited.
.
.
SANbox2 (admin-config) #> config cancel
  Configuration mode will be canceled. Please confirm (y/n): [n] y
SANbox2 (admin) #> admin end
```

The following is an example of how to create a backup file (configdata) and download the file to the workstation.

```
SANbox2 #> admin start
SANbox2 (admin) #> config backup
SANbox2 (admin) #> admin end
SANbox2 #> exit

#>ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> get configdata
ftp> quit
```

The following is an example of how to upload a configuration backup file (configdata) from the workstation to the switch, and then restore the configuration.

```
#> ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> put configdata
ftp> quit

SANbox2 #> admin start
SANbox2 (admin) #> config restore
The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
 Alarm Msg: [Tue Jun 10 09:25:56.938 2003][A1005.0021][SM][Configuration is being
restored -  this could take several minutes !]
  Alarm Msg: [Tue Jun 10 09:26:19.266 2003][A1000.000A][SM][The switch will be
reset in 3 seconds due to a config restore]
SANbox2 (admin) #>
  Alarm Msg: [Tue Jun 10 09:26:22.296 2003][A1000.0005][SM][The switch is being
reset]
Good bye.
```

Date Command

This command displays or sets the system date and time. To set the date and time the information string must be provided in this format: MMDDhhmmCCYY. The new date and time takes effect immediately.

Authority Admin session except to display the date.

Syntax **date**
[MMDDhhmmCCYY]

Keywords ***[MMDDhhmmCCYY]***
Specifies the date – this requires an admin session. If you omit [MMDDhhmmCCYY], the current date is displayed which does not require an admin session.

Examples The following is an example of the Date command:

```
SANbox2 #> date

  Mon Apr 07 07:51:24 2003
```

Fallback Command

Assigns the pending firmware status back and forth between the active and inactive firmware images stored in switch memory.

Authority Admin session

Syntax **fallback**

Notes

- The Show Switch command displays the two firmware images, active firmware, inactive firmware, and pending firmware versions.
- After executing the Fallback command, reset the switch to activate the pending firmware.

Examples The following is an example of the Fallback command:

```
SANbox2 #> admin start

SANbox2 (admin) #> fallback

  Reverting to previous software image.  Please confirm (y/n): [n] y
```

Hardreset Command

Resets the switch and performs a power-on self test. This reset disrupts traffic, activates the pending firmware, and clears the alarm log. To save the alarm log before resetting, refer to the ”Set Log Command” on page A-43.

Authority Admin session

Syntax **hardreset**

Notes To reset the switch without a power-on self test, refer to the ”Reset Command” on page A-25.

To reset the switch without disrupting traffic, refer to the ”Hotreset Command” on page A-18.

Help Command

Displays a brief description of the specified command, its keywords, and usage.

Authority None

Syntax **help *[command] [keyword]***

Keywords ***[command]***
Displays a summary of the command given by [command] and its keywords. If you omit [command], the system displays all available commands.

[keyword]
Displays a summary of the keyword given by [keyword] belonging to the command given by [command]. If you omit [keyword], the system displays the available keywords for the specified command.

all
Displays a list of all available commands (including command variations).

Examples The following is an example of the Help Config command:

```
SANbox2 #> help config
config CONFIG_OPTIONS
The config command operates on configurations.

  Usage: config   { activate | backup   | cancel   | copy     | delete   |
                    edit     | list     | restore  | save }
```

The following is an example of the Help Config Edit command:

```
SANbox2 #> help config edit
config edit [CONFIG_NAME]
This command initiates a configuration session and places the current session
into config edit mode.
If CONFIG_NAME is given and it exists, it gets edited; otherwise, it gets
created.  If it is not given, the currently active configuration is edited.

Admin mode is required for this command.

  Usage: config edit [CONFIG_NAME]
```

History Command

Displays a numbered list of the previously entered commands from which you can re-execute selected commands.

Authority None

Syntax **history**

Notes Use the History command to provide context for the ! command:

- Enter ![command] to re-enter the most recent execution of that command.
- Enter ![line number] to re-execute the corresponding command from the History display
- Enter ![partial command string] to re-execute a command that matches the command string.
- Enter !! to re-execute the most recent command.

Examples The following is an example of the History command:

```
SANbox2 #> history
   1 show switch
   2 date
   3 help set
   4 history

SANbox2 #> !3
help set

set SET_OPTIONS
There are many attributes that can be set.
Type help with one of the following to get more information:

  Usage: set   { alarm     | beacon    | config    | log       | pagebreak |
                 port      | setup     | switch }
```

Hotreset Command

Resets the switch for the purpose of activating the pending firmware without disrupting traffic. This command terminates all management sessions, saves all configuration information, and clears the alarm log. After the pending firmware is activated, the configuration is recovered. This process takes less than 80 seconds. To save the alarm log to a file before resetting, refer to the ”Set Log Command” on page A-43.

Authority Admin session

Syntax **hotreset**

Notes You can load and activate version 4.0.x firmware on an operating switch without disrupting data traffic or having to re-initialize attached devices under the following conditions:

- The current firmware version is a 2.0, 3.0, or a 4.0.x version that precedes the upgrade version.
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, and switch configuration changes.
- No port in the fabric is in the diagnostic state.
- No zoning changes are being made in the fabric.
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.

Ports that are stable when the non-disruptive activation begins, then change states, will be reset. When the non-disruptive activation is complete, SANbox Manager sessions reconnect automatically. However, Telnet sessions must be restarted manually. This command clears the event log and all counters.

Image Command

Manages and installs switch firmware.

Authority Admin session

Syntax

image
cleanup
fetch [account_name] [ip_address] [file_source] [file_destination]
list
unpack [file]

Keywords

cleanup
Removes all firmware image files from the switch. All firmware image files are removed automatically each time the switch is reset.

fetch [account_name] [ip_address] [file_source] [file_destination]
Retrieves image file given by [file_source] and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the FTP server with the IP address given by [ip_address] and an account name given by [account_name]. If an account name needs a password to access the FTP server, the system will prompt you for it.

list
Displays the list of image files that reside on the switch.

unpack [file]
Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch must be reset for the new firmware to take effect.

Notes To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

Use the Hotreset command to perform a non-disruptive activation.

Lip Command

Reinitializes the specified loop port.

Authority Admin session

Syntax **lip [port_number]**

Keywords **[port_number]**
The number of the port to be reinitialized.

Examples The following is an example of the Lip command:

```
SANbox2 (admin) #> lip 2
```

Passwd Command

Changes a user account's password.

Authority Admin account name and an admin session to change another account's password; You can change you own password without an Admin session.

Syntax **passwd [account_name]**

Keywords **[account_name]**
The user account name. To change the password for an account name other than your own, you must open an admin session with the account name Admin. If you omit [account_name], you will be prompted to change the password for the current account name.

Examples The following is an example of the Passwd command:

```
SANbox2 (admin) #> passwd user2

     Press 'q' and the ENTER key to abort this command.

  account OLD password               : ********
  account NEW password (4-20 chars)  : ********

  please confirm account NEW password: ********
  password has been changed.
```

Ping Command

Initiates an attempt to communicate with another switch over an Ethernet network and reports the result.

Authority None

Syntax **ping**
ip_address

Keywords **ip_address**
The IP address of the switch to query.

Examples The following is an example of a successful Ping command:

```
SANbox2 #> ping 10.20.11.57
  Ping command issued. Waiting for response...
SANbox2 #>
  Response successfully received from 10.20.11.57.
```

This following is an example of an unsuccessful Ping command:

```
SANbox2 #> ping 10.20.10.100
  Ping command issued. Waiting for response...
  No response from 10.20.10.100. Unreachable.
```

Ps Command

Displays current system process information.

Authority None

Syntax **ps**

Examples The following is an example of the Ps command:

```
SANbox2 #> ps
PID  PPID %CPU     TIME     ELAPSED COMMAND
338   327  0.0 00:00:00  3-01:18:35 cns
339   327  0.0 00:00:01  3-01:18:35 ens
340   327  0.0 00:00:21  3-01:18:35 dlog
341   327  0.1 00:05:35  3-01:18:35 ds
342   327  0.2 00:11:29  3-01:18:35 mgmtApp
343   327  0.0 00:00:04  3-01:18:35 fc2
344   327  0.0 00:02:16  3-01:18:35 nserver
345   327  0.0 00:02:44  3-01:18:35 mserver
346   327  0.8 00:35:12  3-01:18:35 util
347   327  0.0 00:00:29  3-01:18:35 snmpservicepath
348   327  0.0 00:02:46  3-01:18:34 eport
349   327  0.0 00:00:21  3-01:18:34 PortApp
350   327  5.6 04:08:24  3-01:18:34 port_mon
351   327  0.0 00:01:38  3-01:18:34 zoning
352   327  0.0 00:00:01  3-01:18:34 diagApp
404   327  0.0 00:00:04  3-01:18:27 snmpd
405   327  0.0 00:00:02  3-01:18:27 snmpmain
406   405  0.0 00:00:00  3-01:18:26 snmpmain
```

Quit Command

Closes the Telnet session.

Authority None

Syntax **quit, exit, or logout**

Notes You can also enter Control-D to close the Telnet session.

Reset Command

Resets the switch configuration parameters. If you omit the keyword, the default is Reset Switch.

Authority Admin session

Syntax **reset**

config *[config_name]*
factory
port [port_number]
snmp
switch (default)
system
zoning

Keywords **config *[config_name]***

Resets the configuration given by [config_name] to the factory default values for switch, port, port threshold alarm, and zoning configuration. If [config_name] does not exist on the switch, a configuration with that name will be created. If you omit [config_name], the active configuration is reset. You must activate the configuration for the changes to take effect. Refer to Table A-3 through Table A-6 for switch, port, and port threshold alarm configuration default values.

factory

Resets switch configuration, port configuration, port threshold alarm configuration, zoning configuration, SNMP configuration, system configuration, and zoning to the factory default values. The switch configuration is activated automatically. Refer to Table A-3 through Table A-8.

> ***Note:*** Because this keyword changes network parameters, the workstation could lose communication with the switch and release the Admin session.

port [port_number]

Reinitializes the port given by [port_number]. Ports are numbered beginning with 0.

snmp

Resets the SNMP configuration settings to the factory default values. Refer to Table A-7 for SNMP configuration default values.

switch

Resets the switch without a power-on self test. This is the default. This reset disrupts traffic and does the following:

- Activates the pending firmware.
- Closes all management sessions.

- Clears the alarm log. To save the alarm log before resetting, refer to the "Set Log Command" on page A-43.

To reset the switch with a power-on self test, refer to the "Hardreset Command" on page A-15. To reset the switch without disrupting traffic, refer to the "Hotreset Command" on page A-18.

system
Resets the system configuration settings to the factory default values. Refer to Table A-8 for system configuration default values.

> ***Note:*** Because this keyword changes network parameters, the workstation could lose communication with the switch.

zoning
Clears the zoning database and deactivates the active zone set. The zoning configuration values (autosave, default visibility) remain unchanged.

Notes

The following tables specify the various factory default settings:

Table A-3. Switch Configuration Defaults

Parameter	Default
Admin State	Online
Broadcast Enabled	True
InbandEnabled	True
FDMIEnabled	True
FDMIEntries	1000
Domain ID	1 (0x Hex)
Domain ID Lock	False
Symbolic Name	SANbox2
R_A_TOV	10000
E_D_TOV	2000
Principal Priority	254
Configuration Description	SANbox2-8c/16 FC Switch

Table A-4. Port Configuration Defaults

Parameter	Default
Admin State	Online
Link Speed	Auto
Port Type	GL
Symbolic Name	Port n, where n is the port number
ALFairness	False
DeviceScanEnabled	True
ForceOfflineRSCN	False
ARB_FF	False
InteropCredit	0
ExtCredit	0
FANEnable	True
LCFEnable	False
MFSEnable	True
MSEnable	True
NoClose	False
IOStreamGuard	Disabled
VIEnable	False
PDISCPingEnable	True

Table A-5. Port Threshold Alarm Configuration Defaults

Parameter	Default
ThresholdMonitoringEnabled	False
CRCErrorsMonitoringEnabled RisingTrigger FallingTrigger SampleWindow	True 25 1 10

Table A-5. Port Threshold Alarm Configuration Defaults (Continued)

Parameter	Default
DecodeErrorsMonitoringEnabled	True
RisingTrigger	200
FallingTrigger	0
SampleWindow	10
ISLMonitoringEnabled	True
RisingTrigger	2
FallingTrigger	0
SampleWindow	10
LoginMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10
LogoutMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10
LOSMonitoringEnabled	True
RisingTrigger	100
FallingTrigger	5
SampleWindow	10

Table A-6. Zoning Configuration Defaults

Parameter	Default
FC-SW-2 AutoSave	True
Default Visibility	All

Table A-7. SNMP Configuration Defaults

Parameter	Default
SNMPEnabled	True
Contact	<syscontact undefined>
Location	<sysLocation undefined>
Description	SANbox2-8c/16 FC Switch
Trap [1-5] Address	Trap 1: 10.0.0.254; Traps 2–5: 0.0.0.0

Table A-7. SNMP Configuration Defaults

Parameter	Default
Trap [1-5] Port	162
Trap [1-5] Severity	Warning
Trap [1-5] Version	2
Trap [1-5] Enabled	False
ObjectID	1.3.6.1.4.1.1663.1.1.1.1.14 (SANbox2-8c) 1.3.6.1.4.1.1663.1.1.1.1.11 (SANbox2-16)
AuthFailureTrap	False
ProxyEnabled	True

Table A-8. System Configuration Defaults

Parameter	Default
Ethernet Network Discovery	Static
Ethernet Network IP Address	10.0.0.1
Ethernet Network IP Mask	255.0.0.0
Ethernet Gateway Address	10.0.0.254
Admin Timeout	30 minutes
UserAuthentication	False
LocalLogEnabled	True
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254
Temp Monitoring Warning	65
Temp Monitoring Failure	70
Temp Failure Port Shutdown	False

Set Command

Sets a variety of switch parameters.

Authority Admin session for all keywords except Beacon and Pagebreak which are available without an Admin session.

Syntax

set
alarm clear
beacon [state]
config [option]
log [option]
pagebreak [state]
port [option]
setup [option]
switch [state]

Keywords

alarm clear
Clears the alarm log.

beacon [state]
Enables or disables the flashing of the Logged-In LEDs according to [state]. This keyword does not require an admin session. [state] can be one of the following:

on
Enables the flashing beacon.

off
Disables the flashing beacon.

config [option]
Sets switch, port, port threshold alarm, and zoning configuration parameters. Refer to the ”Set Config Command” on page A-32.

log [option]
Specifies the type of entries to be entered in the event log. Refer to the ”Set Log Command” on page A-43.

pagebreak [state]
Specifies how much information is displayed on the screen at a time according to the value given by [state]. This keyword does not require an admin session. [state] can be one of the following:

on
Limits the display of information to 20 lines at a time. The page break functions affects the following commands: Alias (List, Members), Show (Alarm, Log), Zone (List, Members), Zoneset (List, Zones), Zoning (Active, List).

off
Allows continuous display of information without a break.

port [option]
Sets port state and speed for the specified port. The previous Set Config Port settings are restored after a switch reset or a reactivation of a switch configuration. Refer to the ”Set Port Command” on page A-46.

setup [option]
Changes SNMP and system configuration settings. Refer to the ”Set Setup Command” on page A-48.

switch [state]
Changes the administrative state for all ports on the switch to the state given by [state]. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a switch configuration. [state] can be one of the following:

online
Places all ports online

offline
Places all ports offline.

diagnostics
Prepares all ports for testing.

Examples

The following examples enables and disables the beacon:

```
SANbox2 #> set beacon on

  Command succeeded.

SANbox2 $> set beacon off

  Command succeeded.
```

Set Config Command

Sets switch, port, port threshold alarm, and zoning configuration parameters. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command. Refer to the ”Config Command” on page A-10.

Authority Admin session and a Config Edit session

Syntax **set config**
port *[port_number]*
ports *[port_number]*
switch
threshold
zoning

Keywords **port *[port_number]***
Initiates an edit session in which to change configuration parameters for the port number given by [port_number]. If you omit [port_number], the system begins with port 0 and proceeds in order through the last port. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to end the configuration for one port, or “qq” to end the configuration for all ports. Table A-9 describes the port parameters.

ports *[port_number]*
Initiates an editing session in which to change configuration parameters for all ports based on the configuration for the port given by [port_number]. If you omit [port_number], port 0 is used. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to end the configuration. Table A-9 describes the port parameters.

Table A-9. Set Config Port Parameters

Parameter	Description
AdminState	Port administrative state: ■ Online – Activates and prepares the port to send data. This is the default. ■ Offline – Prevents the port from receiving signal and accepting a device login. ■ Diagnostics – Prepares the port for testing and prevents the port from accepting a device login. ■ Down – Disables the port by removing power from the port lasers.
LinkSpeed	Transmission speed: 1Gbps, 2 Gbps, or Auto. The default is Auto.
PortType	Port type: GL, G, F, FL, Donor. The default is GL.

Table A-9. Set Config Port Parameters (Continued)

Parameter	Description
SymbolicPortName	Descriptive name for the port. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Port n where n is the port number.
ALFairness	Arbitration loop fairness. Enables (True) or disables (False) the switch's priority to arbitrate on the loop. The default is False.
DeviceScanEnabled	Enables (True) or disables (False) the scanning of the connected device for FC-4 descriptor information during login. The default is True.
ForceOfflineRSCN	Enables (False) or disables (True) the immediate transmission of RSCN messages when communication between a port and a device is interrupted. If enabled, the RSCN message is delayed for 200 ms for locally attached devices and 400 ms for devices connected through other switches. The default is False. This parameter is ignored if IOStreamGuard is enabled.
ARB_FF	Send ARB_FF (True) instead of IDLEs (False) on the loop. The default is False.
InteropCredit	Interoperability credit. The number of buffer-to-buffer credits per port. 0 means the default (12) is unchanged. Changing interoperability credits is necessary only for E_Ports that are connected to non-FC-SW-2-compliant switches. Contact your authorized maintenance provider for assistance in using this feature.
ExtCredit	Extended credits. The number of port buffer credits that this port can acquire from donor ports. The default is 0.
FANEnable	Fabric address notification. Enables (True) or disables (False) the communication of the FL_Port address, port name, and node name to the logged-in NL_Port. The default is True.
LCFEnable	Link control frame preference routing. Enables (True) or disables (False) preferred routing of frames with R_CTL = 1100 (Class 2 responses). The default is False. Enabling LCFEnable will disable MFSEnable.

Table A-9. Set Config Port Parameters (Continued)

Parameter	Description
MFSEnable	Multi-Frame Sequence bundling. Prevents (True) or allows (False) the interleaving of frames in a sequence. The default is True. Enabling MFSEnable disables LCFEnable and VIEnable.
MSEnable	Management server enable. Enables (True) or disables (False) management server on this port. The default is True.
NoClose	Loop circuit closure prevention. Enables (True) or disables (False) the loop's ability to remain in the open state indefinitely. True reduces the amount of arbitration on a loop when there is only one device on the loop. The default is False.
IOStreamGuard	I/O Stream Guard. Enable (Enable) or disables (Disable) the suppression of RSCN messages. I/O Stream Guard should be enabled only for ports connected to initiator devices. The default is Disable.
VIEnable	Enables (True) or disables (False) VI preference routing. The default is False. Enabling VIEnable will disable MFSEnable.
PDISCPingEnable	Enables (True) or disables (False) the transmission of ping messages from the switch to all devices on a loop port. The default is True.

switch
Initiates an editing session in which to change switch configuration settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Table A-10 describes the Set Config Switch parameters.

Table A-10. Set Config Switch Parameters

Parameter	Description
AdminState	Switch administrative state: online, offline, or diagnostics. The default is Online.
BroadcastEnabled	Broadcast. Enables (True) or disables (False) forwarding of broadcast frames. The default is True.
InbandEnabled	Inband management. Enables (True) or disables (False) the ability to manage the switch over an ISL. The default is True.
FDMIEnabled	Fabric Device Monitoring Interface. Enables (True) or disables (False) the monitoring of target and initiator device information.
FDMIEntries	The number of device entries to maintain in the FDMI database. Enter a number from 0–1000. The default is 1000.
DefaultDomainID	Default domain ID. The default is 1.
DomainIDLock	Prevents (True) or allows (False) dynamic reassignment of the domain ID. The default is False.
SymbolicName	Descriptive name for the switch. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is SANbox2.
R_A_TOV	Resource Allocation Timeout Value. The number of milliseconds the switch waits to allow two ports to allocate enough resources to establish a link. The default is 10000.

Table A-10. Set Config Switch Parameters (Continued)

Parameter	Description
E_D_TOV	Error Detect Timeout Value. The number of milliseconds a port is to wait for errors to clear. The default is 2000.
PrincipalPriority	The priority used in the FC-SW-2 principal switch selection algorithm. 1 is high, 255 is low. The default is 254.
ConfigDescription	Switch configuration description. The configuration description can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is SANbox2-8c/16 FC Switch.
FC-SW-2 Compliant	Propagates just the active zone set throughout the fabric (True, compliant) or the entire zoning database (False, non-compliant). The default is True.
LegacyAddressFormat	Available only when the FC-SW-2 Compliant parameter is False, this parameter enables (True) or disables (False) the use of legacy address formatting for interoperating with non-FC-SW-2 switches. Refer to ”FC-SW-2 Compliant” on page A-36. The default is False.

threshold

Initiates a configuration session by which to generate and log alarms for selected events. The system displays each event, its triggers, and sampling window one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. These parameters must be saved in a configuration and activated before they will take effect. Refer to the ”Config Command” on page A-10 for information about saving and activating a configuration. Table A-11 describes the Set Config Threshold parameters. The switch will down a port if an alarm condition is not cleared within three consecutive sampling windows (by default 30 seconds). Reset the port to bring it back online. An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling trigger.

Table A-11. Set Config Threshold Parameters

Parameter	Description
Threshold Monitoring Enabled	Master enable/disable parameter for all events. Enables (True) or disables (False) the generation of all enabled event alarms. The default is False.
CRCErrorsMonitoringEnabled DecodeErrorsMonitoringEnabled ISLMonitoringEnabled LoginMonitoringEnabled LogoutMonitoringEnabled LOSMonitoringEnabled	The event type enable/disable parameter. Enables (True) or disables (False) the generation of alarms for each of the following events: ■ CRC errors ■ Decode errors ■ ISL connection count ■ Device login errors ■ Device logout errors ■ Loss-of-signal errors
Rising Trigger	The event count above which a rising trigger alarm is logged. The switch will not generate another rising trigger alarm for that event until the count descends below the falling trigger and again exceeds the rising trigger.
Falling Trigger	The event count below which a falling trigger alarm is logged. The switch will not generate another falling trigger alarm for that event until the count exceeds the rising trigger and descends again below the falling trigger.
Sample Window	The period of time in seconds in which to count events.

zoning
Initiates an editing session in which to change switch zoning attributes. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table A-12. Set Config Zoning Parameters

Parameter	Description
FC-SW-2 AutoSave	Available only when the FC-SW-2 Compliant parameter is True, this parameter enables (True) or disables (False) the saving of changes to active zone set in the switch's permanent memory. Refer to "FC-SW-2 Compliant" on page A-36. The default is True. Disabling the Autosave parameter can be useful to prevent the propagation of zoning information when experimenting with different zoning schemes. However, leaving the Autosave parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the Autosave parameter should be enabled in a production environment.
Default Visibility	Enables (All) or disables (None) communication among the switch's ports/devices and the fabric in the absence of an active zone set. The default is All.

Examples

The following is an example of the Set Config Port command:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
SANbox2 (admin-config) #> set config port 1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  1
  ------------------------

  AdminState    (1=Online, 2=Offline, 3=Diagnostics, 4=Down)       [Online]
  LinkSpeed     (1=1Gb/s, 2=2Gb/s, 3=Auto)                         [Auto  ]
  PortType      (GL / G / F / FL / Donor)                          [GL    ]
  SymPortName   (string, max=32 chars)                             [Port1 ]
  ALFairness    (True / False)                                     [False ]
  DeviceScanEnable (True / False)                                  [True  ]
  ForceOfflineRSCN (True / False)                                  [False ]
  ARB_FF        (True / False)                                     [False ]
  InteropCredit (decimal value, 0-255)                             [0     ]
  ExtCredit     (dec value, increments of 11, non-loop only)       [0     ]
  FANEnable     (True / False)                                     [True  ]
  LCFEnable     (True / False)                                     [False ]
  MFSEnable     (True / False)                                     [False ]
  MSEnable      (True / False)                                     [True  ]
  NoClose       (True / False)                                     [False ]
  IOStreamGuard (Enable / Disable)                                 [Disable]
  VIEnable      (True / False)                                     [False ]
  PDISCPingEnable  (True / False)                                  [True  ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
SANbox2 (admin-config) #>
```

The following is an example of the Set Config Switch command:

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
SANbox2 (admin-config) #> set config switch

  A list of attributes with formatting and default values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  AdminState          (1=Online, 2=Offline, 3=Diagnostics) [Online       ]
  BroadcastEnable     (True / False)                       [False        ]
  InbandEnabled       (True / False)                       [False        ]
  FDMIEnabled         (True / False)                       [True         ]
  FDMIEntries         (decimal value, 0-1000)              [1000         ]
  DefaultDomainID     (decimal value, 1-239)               [11           ]
  DomainIDLock        (True / False)                       [True         ]
  SymbolicName        (string, max=32 chars)               [SANbox2       ]
  R_A_TOV             (decimal value, 100-100000 msec)     [10000        ]
  E_D_TOV             (decimal value, 10-20000 msec)       [2000         ]
  PrincipalPriority   (decimal value, 1-255)               [254          ]
  ConfigDescription   (string, max=32 chars)              [SANbox2-8c/16 FC Switch]
  FC-SW-2 Compliant   (True / False)                       [True         ]
```

The following is an example of the Set Config Threshold command:

```
SANbox2 #> admin start
SANbox2  (admin) #> config edit
SANbox2 (admin-config) #> set config threshold

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

ThresholdMonitoringEnabled     (True / False)              [False     ]

CRCErrorsMonitoringEnabled     (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

DecodeErrorsMonitoringEnabled  (True / False)              [True      ]
```

```
  RisingTrigger               (decimal value, 1-1000)     [200       ]
  FallingTrigger              (decimal value, 0-1000)     [0         ]
  SampleWindow                (decimal value, 1-1000 sec) [10        ]

ISLMonitoringEnabled          (True / False)              [True      ]
  RisingTrigger               (decimal value, 1-1000)     [2         ]
  FallingTrigger              (decimal value, 0-1000)     [0         ]
  SampleWindow                (decimal value, 1-1000 sec) [10        ]

LoginMonitoringEnabled        (True / False)              [True      ]
  RisingTrigger               (decimal value, 1-1000)     [5         ]
  FallingTrigger              (decimal value, 0-1000)     [1         ]
  SampleWindow                (decimal value, 1-1000 sec) [10        ]

LogoutMonitoringEnabled       (True / False)              [True      ]
  RisingTrigger               (decimal value, 1-1000)     [5         ]
  FallingTrigger              (decimal value, 0-1000)     [1         ]
  SampleWindow                (decimal value, 1-1000 sec) [10        ]

LOSMonitoringEnabled          (True / False)               [True     ]
  RisingTrigger               (decimal value, 1-1000)     [100      ]
  FallingTrigger              (decimal value, 0-1000)     [5        ]
  SampleWindow                (decimal value, 1-1000 sec) [10       ]

Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Zoning command.

```
SANbox2 #> admin start
SANbox2 (admin) #> config edit
SANbox2 (admin-config) #> set config zoning

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

  FC-SW-2 AutoSave     (True / False)  [True]
  Default Visibility   (All / None)    [All ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Set Log Command

Specifies the type of entries to be entered in the event log. Log entries are created for ports, components, and event severity levels.

Authority Admin session

Syntax

set log
archive
clear
component [list]
level [level]
port [port_list]
restore
save
start (default)
stop

Keywords

archive
Collects the most recent 200 entries plus the previous 1000 entries and stores the result in new file named *logfile* that is maintained in switch memory where it can be downloaded using FTP. To download *logfile*, open an FTP session, log in with account name/password of “images” for both, and type “get logfile”.

clear
Clears all log entries.

component [list]
Specifies one or more components to monitor for events. Use <space> to delimit values in the list. Choose one or more of the following values:

All
Monitors all components. To maintain optimal switch performance, do not use this setting with the Level keyword set to Info.

Chassis
Monitors chassis hardware components such as fans and power supplies.

Eport
Monitors all E_Ports.

Mgmtserver
Monitors management server status.

Nameserver
Monitors name server status.

None
Monitor none of the component events.

Other
Monitors other miscellaneous events.

Port
Monitors all port events

Switch
Monitors switch management events.

Zoning
Monitors zoning conflict events.

level [level]
Specifies the severity level given by [level] to use in monitoring events for the specified components or ports. [level] can be one of the following values:

Critical
Monitors critical events.

Warn
Monitors warning events.

Info
Monitors informational events. To maintain optimal switch performance, do not use this setting with the Component keyword set to All.

None
Monitors none of the severity levels.

port [port_list]
Specifies one or more ports to monitor for events. Choose one of the following values:

[port_list]
Specifies port or ports to monitor. Use a <space> to delimit values in the list. Ports are numbered beginning with 0.

All
Specifies all ports.

None
Disables monitoring on all ports.

restore
Restores and saves the port, component, and level settings to the default values.

save
Saves the log settings for the component, level, and port. These settings remain in effect after a switch reset. The log settings can be viewed using the Show Log Settings command. To export log entries to a file, use the Set Log Archive command.

start
Starts the logging of events based on the Port, Component, and Level keywords assigned to the current configuration. The logging continues until you enter the Set Log Stop command.

stop
Stops logging of events.

Notes To maintain optimal switch performance, do not set the Component keyword to All and the Level keyword to Info at the same time.

Set Port Command

Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. This command also clears port counters.

Authority Admin session except for the Clear keyword.

Syntax

set port [port_number]
bypass [alpa]
clear
enable
speed [transmission_speed]
state [state]

Keywords

[port_number]
Specifies the port. Ports are numbered beginning with 0.

bypass [alpa]
Sends a Loop Port Bypass (LPB) to a specific Arbitrated Loop Physical Address (ALPA) or to all ALPAs on the arbitrated loop. [alpa] can be a specific ALPA or the keyword ALL to choose all ALPAs.

clear
Clears the counters on the port. This keyword does not require an admin session.

enable
Sends a Loop Port Enable (LPE) to all ALPAs on the arbitrated loop.

speed [transmission_speed]
Specifies the transmission speed for the specified port. Choose one of the following port speed values:

1Gb/s
One gigabit per second.

2Gb/s
Two gigabits per second.

Auto
The port speed is automatically detected.

state [state]
Specifies one of the following administrative states for the specified port:

Online
Places the port online. This activates and prepares the port to send data.

Offline
Places the port offline. This prevents the port from receiving signal and accepting a device login.

Diagnostics
Prepares the port for testing. This prepares the port for testing and prevents the port from accepting a device login.

Down
Disables the port by removing power from the port lasers.

Set Setup Command

Changes SNMP and system configuration settings. The switch maintains one SNMP configuration and one system configuration.

Authority Admin session

Syntax **set setup**
snmp
system

Keywords **snmp**
Prompts you in a line-by-line fashion to change SNMP configuration settings. Table A-13 describes the SNMP fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table A-13. SNMP Configuration Settings

Entry	Description
SNMPEnabled	Enables (True) or disables (False) SNMP on the switch. The default is True.
Contact	Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters excluding #, semicolon (;), and comma (,). The default is undefined.
Location	Specifies the name of the switch location. The name can be up to 64 characters excluding #, semicolon (;), and comma (,). The default is undefined.
Trap [1-5] Address	Specifies the workstation IP address to which SNMP traps are sent. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0. Addresses, other than 0.0.0.0, for all traps must be unique.
Trap [1-5] Port	Specifies the workstation port to which SNMP traps are sent. Valid workstation port numbers are 1–65535. The default is 162.
Trap [1-5] Severity	Specifies the severity level to use when monitoring trap events. The default is Warning
Trap [1-5] Version	Specifies the SNMP version (1 or 2) to use in formatting traps. The default is 2.
Trap [1-5] Enabled	Specifies whether traps (event information) are enabled or disabled (default).

Table A-13. SNMP Configuration Settings (Continued)

Entry	Description
ReadCommunity	Read community password that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The read community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “public”.
WriteCommunity	Write community password that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The write community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “private”.
TrapCommunity	Trap community password that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The trap community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “public”.
AuthFailureTrap	Enables (True) or disables (False) the generation of traps in response to trap authentication failures. The default is False.
ProxyEnabled	Enables (True) or disables (False) SNMP communication with other switches in the fabric. The default is True.

system
Prompts you in a line-by-line fashion to change system configuration settings. Table A-14 describes the system configuration fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Note: Changing the IP address will terminate all Ethernet management sessions.

Table A-14. System Configuration Settings

Entry	Description
Eth0NetworkDiscovery	Ethernet boot method: 1 - Static, 2 - Bootp, 3 - DHCP, 4 - RARP. The default is 1 - Static.
Eth0NetworkAddress	Ethernet Internet Protocol (IP) address. The default is 10.0.0.1.

Table A-14. System Configuration Settings (Continued)

Entry	Description
Eth0NetworkMask	Ethernet subnet mask address.
Eth0GatewayAddress	Ethernet IP address gateway.
AdminTimeout	Specifies the amount of time in minutes the switch waits before terminating an idle Admin session. Zero (0) disables the time out threshold. The default is 30, the maximum is 1440.
TempMonitoringWarning	Warning temperature threshold in °C above which a warning condition alarm is generated. The default is 65 °C.
TempMonitoringFailure	Failure temperature threshold in °C above which a failure condition alarm is generated. The default is 70 °C.
TempFailurePortShutdown	Enables (True) or disables (False) the switch's ability to place all ports down when the internal temperature exceeds the failure threshold. The default is False. If the temperature exceeds the failure threshold, correct the problem, then reset the switch to bring the ports back online.
UserAuthentication	Enables (True) or disables (False) the enforcement of account names and passwords for SANbox Manager. The default is False.
LocalLogEnabled	Enables (True) or disables (False) the saving of log information on the switch. The default is True.
RemoteLogEnabled	Enables (True) or disables (False) the recording of the switch event log on a remote host that supports the syslog protocol. The default is False.
RemoteLogHostAddress	The IP address of the host that will receive the switch event log information if remote logging is enabled. The default is 10.0.0.254.

Examples

The following is an example of the Set Setup SNMP command:

```
SANbox2 #> admin start
SANbox2 (admin) #> set setup snmp
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
```

```
Trap Severity Options
---------------------
unknown, emergency, alert, critical, error, warning, notify, info, debug, mark

SNMPEnabled         (True / False)               [True             ]
Contact             (string, max=64 chars)      [<sysContact undefined]
Location            (string, max=64 chars)      [sysLocation undefined]
Trap1Address        (dot-notated IP Address)    [10.20.71.15      ]
Trap1Port           (decimal value)             [162              ]
Trap1Severity       (see allowed options above) [warning          ]
Trap1Version        (1 / 2)                     [2                ]
Trap1Enabled        (True / False)              [False            ]
Trap2Address        (dot-notated IP Address)    [0.0.0.0          ]
Trap2Port           (decimal value)             [162              ]
Trap2Severity       (see allowed options above) [warning          ]
Trap2Version        (1 / 2)                     [2                ]
Trap2Enabled        (True / False)              [False            ]
Trap3Address        (dot-notated IP Address)    [0.0.0.0          ]
Trap3Port           (decimal value)             [162              ]
Trap3Severity       (see allowed options above) [warning          ]
Trap3Version        (1 / 2)                     [2                ]
Trap3Enabled        (True / False)              [False            ]
Trap4Address        (dot-notated IP Address)    [0.0.0.0          ]
Trap4Port           (decimal value)             [162              ]
Trap4Severity       (see allowed options above) [warning          ]
Trap4Version        (1 / 2)                     [2                ]
Trap4Enabled        (True / False)              [False            ]
Trap5Address        (dot-notated IP Address)    [0.0.0.0          ]
Trap5Port           (decimal value)             [162              ]
Trap5Severity       (see allowed options above) [warning          ]
Trap5Version        (1 / 2)                     [2                ]
Trap5Enabled        (True / False)              [False            ]
ReadCommunity       (string, max=32 chars)      [public           ]
WriteCommunity      (string, max=32 chars)      [private          ]
TrapCommunity       (string, max=32 chars)      [public           ]
AuthFailureTrap     (True / False)              [False            ]
ProxyEnabled        (True / False)              [True             ]
```

The following is an example of the Set Setup System command:

```
SANbox2 (admin) #> set setup system
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

Eth0NetworkDiscovery    (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp)  [Static       ]
Eth0NetworkAddress      (dot-notated IP Address)             [10.0.0.1     ]
Eth0NetworkMask         (dot-notated IP Address)             [255.255.255.0]
Eth0GatewayAddress      (dot-notated IP Address)             [10.0.0.254   ]
AdminTimeout            (dec value 0-1440 minutes, 0=never)  [30           ]
TempMonitoringWarning   (dec value 0-100 degrees Celsius)    [65           ]
TempMonitoringFailure   (dec value 0-100 degrees Celsius)    [70           ]
TempFailurePortShutdown (True / False)                       [False        ]
UserAuthentication      (True / False)                       [False        ]
LocalLogEnabled         (True / False)                       [True         ]
RemoteLogEnabled        (True / False)                       [False        ]
RemoteLogHostAddress    (dot-notated IP Address)             [10.0.0.254   ]
```

Show Command

Displays fabric, switch, and port operational information.

Authority None

Syntax **show**

about
alarm
broadcast
chassis
config [option]
domains
donor
fabric
fdmi *[node_wwn]*
interface
log *[option]*
lsdb
mem [count]
ns *[option]*
pagebreak
perf *[option]*
port *[port_number]*
post log
setup [option]
steering *[domain_id]*
support
switch
topology
users
version

Keywords

about
Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the Version keyword.

alarm
Displays the last 200 alarm entries. The alarm log is cleared when the switch is reset or power cycled.

broadcast
Displays the broadcast tree information and all ports that are currently transmitting and receiving broadcast frames.

chassis
Displays chassis component status and temperature.

config [option]
Displays switch, port, and zoning configuration attributes. Refer to the "Show Config Command" on page A-65.

domains
Displays list of each domain and its worldwide name in the fabric.

donor
Displays list of current donor configuration for all ports.

fabric
Displays list of each domain, symbolic name, worldwide name, node IP address, and port IP address.

fdmi ***[node_wwn]***
Displays information (worldwide name, manufacturer, model, and number of ports) for the device host bus adapter given by [node_wwn]. If you omit [node_wwn], the command displays host bus adapter information for all attached devices. Illegal characters in the display appear as question marks (?).

interface
Displays the status of the active network interfaces.

log ***[option]***
Displays log entries. Refer to the "Show Log Command" on page A-68. The log is cleared when the switch is reset or power cycled.

lsdb
Displays Link State database information

mem [count]
Displays information about memory activity for the number of seconds given by [count]. If you omit [count], the value 1 is used. Displayed memory values are in 1K block units.

> ***Note:*** This keyword will display memory activity updates until [count] is reached – it cannot be interrupted. Therefore, avoid using large values for [count].

ns ***[option]***
Displays name server information for the specified [option]. If you omit [option], name server information for the local domain ID is displayed. [option] can have the following values:

all
Displays name server information for all switches and ports.

[domain_id]
Displays name server information for the switch given by [domain_id]. [domain_id] is a switch domain ID.

[port_id]
Displays name server information for the port given by [port_id]. [port_id] is a port Fibre Channel address.

pagebreak
Displays the current pagebreak setting. The pagebreak setting limits the display of information to 20 lines (On) or allows the continuous display of information without a break (Off).

perf *[option]*
Displays performance information for all ports. Refer to the "Show Perf Command" on page A-71.

port *[port_number]*
Displays operational information for the port given by [port_number]. Ports are numbered beginning with 0. If [port number] is omitted, information is displayed for all ports. Table A-15 describes the port parameters.

Table A-15. Show Port Parameters

Entry	Description
AlInit	Incremented each time the port begins AL initialization.
AlInitError	Number of times the port entered initialization and the initialization failed.
Bad Frames	Number of frames that have framing errors.
ClassXFramesIn	Number of class *x* frames received by this port.
ClassXFramesOut	Number of class *x* frames sent by this port.
ClassXWordsIn	Number of class *x* words received by this port.
ClassXWordsOut	Number of class *x* words sent by this port.
ClassXToss	Number of times an SOFi3 or SOFn3 frame is tossed from TBUF.
DecodeError	Number of decode errors detected
EpConnects	Number of times an E_Port connected through ISL negotiation.
FBusy	Number of times the switch sent a F_BSY because Class 2 frame could not be delivered within ED_TOV time. Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_Port that is preventing delivery of this frame.
Flowerrors	Received a frame when there were no available credits.

Table A-15. Show Port Parameters (Continued)

Entry	Description
FReject	Number of frames from devices that were rejected.
InvalidCRC	Invalid CRC detected.
InvalidDestAddr	Invalid destination address detected.
LIP_AL_PD_ALPS	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.
LIP_F7_AL_PS	This LIP is used to reinitialize the loop. An L_Port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.
LIP_F8_AL_PS	This LIP denotes a loop failure detected by the L_Port identified by AL_PS.
LIP_F7_F7	A loop initialization primitive frame used to acquire a valid AL_PA.
LIP_F8_F7	A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or a loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
Login	Number of device logins
Logout	Number of device logouts
LoopTimeouts	A two (2) second timeout as specified by FC-AL-2.
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
PrimSeqErrors	Primitive sequence errors detected.
RxLinkResets	Number of link reset primitives received from an attached device.
RxOfflineSeq	Number of offline sequences received. An OLS is issued for link initialization, a Receive & Recognize Not_Operational (NOS) state, or to enter the offline state.
TotalErrors	Total number of errors detected.

Table A-15. Show Port Parameters (Continued)

Entry	Description
TotalLIPsRecvd	Number of loop initialization primitive frames received by this port.
TotalLIPsXmitd	Number of loop initialization primitive frames transmitted by this port.
TotalLinkResets	Total number of link reset primitives.
TotalOfflineSeq	Total number of Offline Sequences issued and received by this port.
TotalRxFrames	Total number of frames received by this port.
TotalRxWords	Total number of words received by this port.
TotalTxFrames	Total number of frames issued by this port.
TotalTxWords	Total number of words issued by this port.
TxLinkResets	Number of Link Resets issued by this port.
TxOfflineSeq	Total number of Offline Sequences issued by this port.

post log
Displays the Power On Self Test (POST) log which contains results from the POST.

setup [option]
Displays setup attributes for the system, SNMP, and the switch manufacturer. Refer to the ”Show Setup Command” on page A-73.

steering *[domain_id]*
Displays the routes that data takes to the switch given by [domain_id]. If you omit [domain_id], the system displays routes for all switches in the fabric.

support
Executes a series of commands that display a complete description of the switch, its configuration, and operation. The display can be captured from the screen and used for diagnosing problems. This keyword is intended for use at the request of your authorized maintenance provider. The commands that are executed include the following:

- Alias List
- Config List
- Date
- History

- Ps
- Show (About, Alarm, Backtrace, Chassis, Config Port, Config Switch, Config Threshold, Dev, Dev Settings, Domains, Donor, Fabric, Log, Log Settings, Lsdb, Mem, Ns, Perf, Port, Setup Mfg, Setup Snmp, Setup System, Steering, Switch, Topology, Users)
- Uptime
- User Accounts
- Whoami
- Zoneset (Active, List)
- Zoning (History, Limits, List)

switch
Displays switch operational information.

topology
Displays all connected devices.

users
Displays a list of logged-in users. This is equivalent to the User List command.

version
Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the About keyword.

Examples

The following is an example of the Show Chassis command:

```
SANbox2 #> show chassis
  Chassis Information
  -------------------
  BoardTemp (1) - Degrees Celsius   32
  BoardTemp (2) - Degrees Celsius   36
  FanStatus (1)                     Good
  FanStatus (2)                     Good
  PowerSupplyStatus (1)             Good
  PowerSupplyStatus (2)             Good
  HeartBeatCode                     1
  HeartBeatStatus                   Normal
```

The following is an example of the Show Domains command:

```
SANbox2 #> show domains
  Principal switch is (remote): 10:00:00:60:69:50:0b:6c
  Upstream Principal ISL is   : 1
  Domain ID List:
        Domain 97  (0x61)  WWN = 10:00:00:c0:dd:00:71:ed
        Domain 98  (0x62)  WWN = 10:00:00:60:df:22:2e:0c
        Domain 99  (0x63)  WWN = 10:00:00:c0:dd:00:72:45
```

```
        Domain 100 (0x64)  WWN = 10:00:00:c0:dd:00:ba:68
        Domain 101 (0x65)  WWN = 10:00:00:60:df:22:2e:06
        Domain 102 (0x66)  WWN = 10:00:00:c0:dd:00:90:ef
        Domain 103 (0x67)  WWN = 10:00:00:60:69:50:0b:6c
        Domain 104 (0x68)  WWN = 10:00:00:c0:dd:00:b8:b7
```

The following is an example of the Show Fabric command:

```
SANbox2 #> show fabric

 Domain     WWN                     Enet IP Addr    FC IP Addr      SymbolicName
 ------     ---                     ------------    ----------      ------------
 16 (0x10)  10:00:00:c0:dd:00:77:81 10.20.68.11     0.0.0.0         gui sb1 .11
 17 (0x11)  10:00:00:c0:dd:00:6a:2d 10.20.68.12     0.0.0.0         sw12
 18 (0x12)  10:00:00:c0:dd:00:c3:04 10.20.68.160    0.0.0.0         sw .160
 19 (0x13)  10:00:00:c0:dd:00:bc:56 10.20.68.108    0.0.0.0         Sb2 .108
```

The following is an example of the Show FDMI command:

```
SANbox2 #> show fdmi

HBA ID                  Manufacturer Model     Ports
--------                ---------------        ------- -----
20:00:00:00:c9:25:9b:96 Emulex Network Systems LP9000  2
20:00:00:00:ca:25:9b:96 QLogic Corporation     QL2330  2
```

The following is an example of the Show FDMI WWN command:

```
SANbox2 #> show fdmi 21:00:00:e0:8b:09:3b:17
  FDMI Information
  -----------------
  Manufacturer                    QLogic Corporation
  SerialNumber                    95923
  Model                           QCP2340
  ModelDescription
  NodeWWN                         20:00:00:e0:8b:09:3b:17
  HardwareVersion                 A
  DriverVersion                   4.12 Beta 21
  OptionRomVersion
  FirmwareVersion                 3.2.15
  OSSystemName                    SunOS 5.8
  MaximumCTPayload
  NumberOfPorts                   1

  Port  21:00:00:e0:8b:09:3b:17
```

```
  SupportedFC4Types                FCP
  SupportedSpeed                   2Gb/s
  CurrentSpeed                     2Gb/s
  MaximumFrameSize                 2048
  OSDeviceName                     qla2300(0)
```

The following is an example of the Show NS (local domain) command:

```
SANbox2 #> show ns
  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   19 (0x13) 1301e1 NL   3   21:00:00:20:37:73:13:69 20:00:00:20:37:73:13:69
  2   19 (0x13) 1301e2 NL   3   21:00:00:20:37:73:12:9b 20:00:00:20:37:73:12:9b
  3   19 (0x13) 1301e4 NL   3   21:00:00:20:37:73:05:26 20:00:00:20:37:73:05:26
  4   19 (0x13) 130d00 N    3   21:01:00:e0:8b:27:a7:bc 20:01:00:e0:8b:27:a7:bc
```

The following is an example of the Show NS [domain_ID] command:

```
SANbox2 #> show ns 18
    Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   18 (0x12) 120700 N    3   21:00:00:e0:8b:07:a7:bc 20:00:00:e0:8b:07:a7:bc
```

The following is an example of the Show NS [port_ID] command:

```
SANbox2 #> show ns 1301e1
  Port ID: 1301e1
  --------
  PortType          NL
  PortWWN           21:00:00:20:37:73:13:69
  SymbolicPortName
  NodeWWN           20:00:00:20:37:73:13:69
  SymbolicNodeName
  NodeIPAddress     0.0.0.0
  ClassOfService    3
  PortIPAddress     0.0.0.0
  FabricPortName    20:01:00:c0:dd:00:bc:56
  FC4Type           FCP
  FC4Desc           (NULL)
```

The following is an example of the Show Interface command:

```
SANbox2 #> show interface
eth0      Link encap:Ethernet  HWaddr 00:C0:DD:00:BD:ED
          inet addr:10.20.68.107  Bcast:10.20.68.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4712 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3000 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:415313 (405.5 Kb)  TX bytes:716751 (699.9 Kb)
          Interrupt:11 Base address:0xfcc0
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:304 errors:0 dropped:0 overruns:0 frame:0
          TX packets:304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20116 (19.6 Kb)  TX bytes:20116 (19.6 Kb)
```

The following is an example of the Show Port command:

```
SANbox2 #> show port 1
    Port Number: 1
  ------------
  AdminState       Online              PortID           150100
  AsicNumber       0                   PortWWN          20:01:00:c0:dd:00:bc:b8
  AsicPort         1                   RunningType      Unknown
  ConfigType       G                   SFPPartNumber    Unknown
  DiagStatus       Passed              SFPRevision      0
  EpConnState      None                SFPType          NotInstalled
  EpIsoReason      NotApplicable       SFPVendor        Unknown
  LinkSpeed        2Gb/s               SFPVendorID      00000000
  LinkState        Inactive            SymbolicName     Port1
  LoginStatus      NotLoggedIn         SyncStatus       SyncLost
  MaxCredit        12                  XmitterEnabled   True
  OperationalState Offline

  ALInit          0                     LIP_F8_AL_PS    0
  ALInitError     0                     LIP_F8_F7       0
  BadFrames       0                     LinkFailures    26
  Class2FramesIn  0                     Login           25
  Class2FramesOut 0                     Logout          24
  Class2WordsIn   0                     LoopTimeouts    0
  Class2WordsOut  0                     LossOfSync      1
```

```
Class3FramesIn  0                    PrimSeqErrors   0
Class3FramesOut 0                    RxLinkResets    23
Class3Toss      0                    RxOfflineSeq    45
Class3WordsIn   0                    TotalErrors     26
Class3WordsOut  0                    TotalLIPsRecvd  0
DecodeErrors    0                    TotalLIPsXmitd  0
EpConnects      25                   TotalLinkResets 77
FBusy           0                    TotalOfflineSeq 59
FlowErrors      0                    TotalRxFrames   0
FReject         0                    TotalRxWords    0
InvalidCRC      0                    TotalTxFrames   0
InvalidDestAddr 0                    TotalTxWords    0
LIP_AL_PD_AL_PS 0                    TxLinkResets    54
LIP_F7_AL_PS    0                    TxOfflineSeq    14
LIP_F7_F7       0
```

The following is an example of the Show Switch command:

```
SANbox2 #> show switch
Switch Information
------------------
SymbolicName                        sw .108
SwitchWWN                           100000c0dd00bc56
SwitchType                          SANbox2-8c/16
BootVersion                         V1.0.0.7-0 (Mon Nov  3 13:11:08 2003)
CreditPool                          0
DomainID                            19 (0x13)
FirstPortAddress                    130000
FlashSize - MBytes                  128
LogLevel                            Critical
MaxPorts                            16
NumberOfResets                      224
ReasonForLastReset                  PowerUp
SWImageVersion (1) - build date     V4.0.0.0-17 (day month date time year)
SWImageVersion (2) - build date     V4.0.0.0-17 (day month date time year)
ActiveImageVersion - build date     V4.0.0.0-2 (day month date time year)
PendingImageVersion - build date    V4.0.0.0-17 (day month date time year)
ActiveConfiguration                 default
AdminState                          Online
AdminModeActive                     False
BeaconOnStatus                      False
OperationalState                    Online
PrincipalSwitchRole                 False
BoardTemp (1) - Degrees Celsius     32
```

```
  BoardTemp (2) - Degrees Celsius   36
  SwitchDiagnosticsStatus           Passed
  SwitchTemperatureStatus           Normal
```

The following is an example of the Show Topology command:

```
SANbox2 #> show topology
Unique ID Key
-------------
A = ALPA,  D = Domain ID,  P = Port ID
Port   Local Local                    Remote  Remote                    Unique
Number Type  PortWWN                  Type    NodeWWN                   ID
------ ----- -------                  ------  -------                   ------
5      F     20:05:00:c0:dd:00:bd:ec   N      20:00:00:00:c9:22:1e:93   010500 P
10     E     20:0a:00:c0:dd:00:bd:ec   E      10:00:00:c0:dd:00:80:21   4(0x4) D
```

The following is an example of the Show Topology command for port 1:

```
SANbox2  #> show topology 1
  Local Link Information
  ----------------------
  PortNumber 1
  PortID     650100
  PortWWN    20:01:00:c0:dd:00:91:11
  PortType   F

Remote Link Information
-----------------------
Device 0
NodeWWN 50:80:02:00:00:06:d5:38
PortType NL
Description (NULL)
IPAddress 0.0.0.0

Device 1
NodeWWN 20:00:00:20:37:2b:08:c9
PortType NL
Description (NULL)
IPAddress 0.0.0.0

Device 2
Description (NULL)
IPAddress 0.0.0.0

Device 3
```

```
NodeWWN 20:00:00:20:37:2b:05:c9
PortType NL
Description (NULL)
IPAddress 0.0.0.0
```

The following is an example of the Show Version command:

```
SANbox2 #> show version
       ************************************************
       *                                              *
       *       Command Line Interface SHell  (CLISH)  *
       *                                              *
       ************************************************

       SystemDescription  SANbox2-8c/16 FC Switch
       Eth0NetworkAddress 10.20.11.192 (use 'set setup system' to update)
       MACAddress         00:c0:dd:00:71:ee
       WorldWideName      10:00:00:c0:dd:00:71:ed
       SerialNumber       FAM033100024
       SymbolicName       SANbox2
       ActiveSWVersion    V4.0.0.0-26
       ActiveTimestamp    day month date time year
       DiagnosticsStatus  Passed
       UserAuthentication True
```

Show Config Command

Displays switch, port, alarm threshold, and zoning for the current configuration.

Authority None

Syntax **show config**
port *[port_number]*
switch
threshold
zoning

Keywords **port *[port_number]***
Displays configuration parameters for the port number given by [port_number]. Ports are numbered beginning with 0. If [port_number] is omitted, all ports are specified.

switch
Displays configuration parameters for the switch.

threshold
Displays alarm threshold parameters for the switch.

zoning
Displays zoning configuration parameters for the switch.

Examples The following is an example of the Show Config Port command:

```
SANbox2 #> show config port 3
    Port Number: 3
  ------------
  AdminState         Offline
  LinkSpeed          Auto
  PortType           GL
  SymbolicName       Port3
  ALFairness         False
  DeviceScanEnabled  True
  ForceOfflineRSCN   False
  ARB_FF             False
  InteropCredit      0
  ExtCredit          0
  FANEnabled         True
  LCFEnabled         False
  MFSEnabled         True
  MSEnabled          True
  NoClose            False
  IOStreamGuard      Disabled
  VIEnabled          False
  PDISCPingEnable    True
```

The following is an example of the Show Config Switch command:

```
SANbox2 #> show config switch
 Configuration Name: default
 -------------------
  Switch Configuration Information
  --------------------------------
  AdminState            Online
  BroadcastEnabled      False
  InbandEnabled         True
  FDMIEnabled           False
  FDMIEntries           10
  DomainID              19 (0x13)
  DomainIDLock          True
  SymbolicName          sw108
  R_A_TOV               10000
  E_D_TOV               2000
  PrincipalPriority     254
  ConfigDescription     SANbox2-8c/16 FC Switch
  ConfigLastSavedBy     admin@OB-session5
  ConfigLastSavedOn     day month date time year
  FC-SW-2 Compliant     True
  Legacy Address Format False[1]
```

The following is an example of the Show Config Threshold command:

```
SANbox2 #> show config threshold
Configuration Name: default
------------

Threshold Configuration Information
-----------------------------------
ThresholdMonitoringEnabled    False
CRCErrorsMonitoringEnabled    True
RisingTrigger                 25
FallingTrigger                1
SampleWindow                  10
DecodeErrorsMonitoringEnabled True
RisingTrigger                 25
FallingTrigger                0
SampleWindow                  10
ISLMonitoringEnabled          True
```

[1] Appears only if FC-SW-2 Compliant is False.

```
  RisingTrigger                2
  FallingTrigger               0
  SampleWindow                 10
  LoginMonitoringEnabled       True
  RisingTrigger                5
  FallingTrigger               1
  SampleWindow                 10
  LogoutMonitoringEnabled      True
  RisingTrigger                5
  FallingTrigger               1
  SampleWindow                 10
  LOSMonitoringEnabled         True
  RisingTrigger                100
  FallingTrigger               5
  SampleWindow                 10
```

The following is an example of the Show Config Zoning command:

```
SANbox2 #> show config zoning

 Configuration Name: default
  -------------------

  Zoning Configuration Information
  --------------------------------
  FC-SW-2 AutoSave      True
  Default Visibility    All
```

Show Log Command

Displays the contents of the log or the parameters used to create entries in the log. The log contains a maximum of 200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority None

Syntax **show log**
component
level
options
port
settings

Keywords **component**
Displays the components currently being monitored for events. The components are as follows:

All
Monitors all components.

Chassis
Monitors chassis hardware components such as fans and power supplies.

Eport
Monitors all E_Ports.

Mgmtserver
Monitors management server status.

Nameserver
Monitors name server status.

None
Monitor none of the component events.

Other
Monitors other miscellaneous events.

Port
Monitors all port events

Switch
Monitors switch management events.

Zoning
Monitors zoning conflict events.

level
Displays the event severity level needed to create an entry in the log. If the severity level occurs on a port or on a component which is not defined, no entry is made in the log. The severity levels are as follows:

Critical
Monitors critical events.

Warn
Monitors warning events.

Info
Monitors informational events.

None
Monitors none of the severity levels.

options
Displays the options used to set the component and severity level attributes.

port
Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but not on a defined port, no entry is made in the log.

settings
Displays the current settings for component, level and port. This command is equivalent to executing the following commands separately: Show Log Component, Show Log Level, and Show Log Port.

Examples

The following is an example of the Show Log Component command:

```
SANbox2 #> show log component


  Current setting(s) for log component: NameServer
```

The following is an example of the Show Log Level command:

```
SANbox2 #> show log level
  Current settings for log
  ------------------------
  level      Critical
```

The following is an example of the Show Log Options command:

```
SANbox2 #> show log options
  Allowed options for log
  -----------------------
  component  All, None, NameServer, MgmtServer, Zoning, Switch, Chassis, Blade,
              Port, Eport, Snmp, Other,CimServer
  level       Critical,Warn,Info,None
```

The following is an example of the Show Log command:

```
SANbox2 #> show log
 [327][day month date time year][I][Eport Port:0/8][Eport State=
E_A0_GET_DOMAIN_ID]
 [328][day month date time year][I][Eport Port: 0/8][FSPF PortUp state=0]
 [329][day month date time year][I][Eport Port: 0/8][Sending init hello]
 [330][day month date time year][I][Eport Port: 0/8][Processing EFP, oxid= 0x8]
 [331][day month date time year][I][Eport Port: 0/8][Eport State = E_A2_IDLE]
 [332][day month date time year][I][Eport Port: 0/8][EFP,WWN= 0x100000c0dd00b845,
len= 0x30]
 [333][day month date time year][I][Eport Port: 0/8][Sending LSU oxid=0xc:type=1]
 [334][day month date time year][I][Eport Port: 0/8][Send Zone Merge Request]
 [335][day month date time year][I][Eport Port: 0/8][LSDB Xchg timer set]
 [336][day month date time year][I][Eport Port: 0/8][Setting attribute
Oper.UserPort.0.8.EpConnState Connected]
```

Show Perf Command

Displays port performance in frames/second and bytes/second. If you omit the keyword, the command displays data transmitted (out), data received (in), and total data transmitted and received in frames/second and bytes per second.

Authority None

Syntax **show perf**
byte
inbyte
outbyte
frame
inframe
outframe
errors

Keywords

byte
Displays continuous performance data in total bytes/second transmitted and received for all ports. Type “q” and press the Enter key to stop the display.

inbyte
Displays continuous performance data in bytes/second received for all ports. Type “q” and press the Enter key to stop the display.

outbyte
Displays continuous performance data in bytes/second transmitted for all ports. Type “q” and press the Enter key to stop the display.

frame
Displays continuous performance data in total frames/second transmitted and received for all ports. Type “q” and press the Enter key to stop the display.

inframe
Displays continuous performance data in frames/second received for all ports. Type “q” and press the Enter key to stop the display.

outframe
Displays continuous performance data in frames/second transmitted for all ports. Type “q” and press the Enter key to stop the display.

errors
Displays continuous error counts for all ports. Type “q” and press the Enter key to stop the display.

Examples The following is an example of the Show Perf command:

```
SANbox2 #> show perf
Port   Bytes/s    Bytes/s    Bytes/s    Frames/s   Frames/s   Frames/s
  Number   (in)       (out)    (total)      (in)       (out)    (total)
  ------ -------    -------    -------    --------   --------   --------
  0      7K         136M       136M       245        68K        68K
  1      58K        0          58K        1K         0          1K
```

```
  2      0          0          0          0          0          0
  3      0          0          0          0          0          0
  4      0          0          0          0          0          0
  5      0          0          0          0          0          0
  6      0          7K         7K         0          245        245
  7      136M       58K        136M       68K        1K         70K
  8      7K         136M       136M       245        68K        68K
  9      58K        0          58K        1K         0          1K
  10     0          0          0          0          0          0
  11     0          0          0          0          0          0
  12     0          0          0          0          0          0
  13     0          0          0          0          0          0
  14     0          7K         7K         0          245        245
  15     136M       58K        136M       68K        1K         70K
```

The following is an example of the Show Perf Byte command:

```
SANbox2 #> show perf byte
Displaying bytes/sec (total)...  (Press 'q' and the ENTER key to stop display)

  0    1    2    3    4    5    6    7    8    9    10   11   12   13   14   15
  ------------------------------------------------------------------------------
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    8K   136M
  0    0    0    0    0    0    0    0    135M 58K  0    0    0    0    7K   135M
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    7K   136M
  0    0    0    0    0    0    0    0    137M 58K  0    0    0    0    8K   137M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    8K   136M
  0    0    0    0    0    0    0    0    136M 58K  0    0    0    0    7K   136M
q
```

Show Setup Command

Displays the current SNMP and system settings.

Authority None

Syntax **show setup**
mfg
snmp
system

Keywords **mfg**
Displays manufacturing information about the switch.

snmp
Displays the current SNMP settings.

system
Displays the current system settings.

Examples The following is an example of the Show Setup Mfg command:

```
SANbox2 #> show setup mfg
  Manufacturing Information
  -------------------------
  BrandName                QLogic Corporation
  BuildDate                Unknown
  ChassisPartNumber        Unknown
  ChassisSerialNumber      0
  CPUBoardSerialNumber     000603949
  MACAddress               00:c0:dd:00:90:aa
  PlanarPartNumber         Unknown
  SwitchSymbolicName       SANbox2
  SwitchWWN                10:00:00:c0:dd:00:90:ab
  SystemDescription        SANbox2-8c/16 FC Switch
  SystemObjectID           1.3.6.1.4.1.1663.1.1.1.1.11
```

The following is an example of the Show Setup Snmp command:

```
SANbox2 #> show setup snmp
  SNMP Information
  ----------------
  SNMPEnabled           True
  Contact               <sysContact undefined>
  Location              N_107 System Test Lab
  Description           SANbox2-8c/16 FC Switch
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Version          2
```

```
  Trap1Enabled          False
  Trap2Address          0.0.0.0
  Trap2Port             162
  Trap2Severity         warning
  Trap2Version          2
  Trap2Enabled          False
  Trap3Address          0.0.0.0
  Trap3Port             162
  Trap3Severity         warning
  Trap3Version          2
  Trap3Enabled          False
  Trap4Address          0.0.0.0
  Trap4Port             162
  Trap4Severity         warning
  Trap4Version          2
  Trap4Enabled          False
  Trap5Address          0.0.0.0
  Trap5Port             162
  Trap5Severity         warning
  Trap5Version          2
  Trap5Enabled          False
  ObjectID              1.3.6.1.4.1.1663.1.1.1.1.11
  AuthFailureTrap       True
  ProxyEnabled          True
```

The following is an example of the Show Setup System command:

```
SANbox2 #> show setup system
  System Information
  ------------------
  Eth0NetworkDiscovery     Static
  Eth0NetworkAddress       10.20.11.32
  Eth0NetworkMask          255.255.252.0
  Eth0GatewayAddress       10.20.8.254
  AdminTimeout             30
  TempMonitoringWarning    65
  TempMonitoringFailure    70
  TempFailurePortShutdown  False
  UserAuthentication       False
  LocalLogEnabled          True
  RemoteLogEnabled         False
  RemoteLogHostAddress     10.0.0.254
```

Shutdown Command

Terminates all data transfers on the switch at convenient points and closes the Telnet session. Always power cycle the switch after entering this command.

Authority Admin session

Syntax **shutdown**

Notes Always use this command to perform an orderly shut down before removing power from the switch.

When the shutdown is complete, the Heartbeat LED is extinguished.

Test Command

Tests ports using internal (SerDes level), external (transceiver), and online loopback tests. Internal and external tests require that the port be placed in diagnostic mode. Refer to the "Set Command" on page A-30 for information about changing the port administrative state. While the test is running, the remaining ports on the switch remain fully operational.

Authority Admin session

Syntax **test**

port [port_number] [test_type]
cancel
status

Keywords **port [port_number] *[test_type]***
Tests the port given by [port_number] using the test given by [test_type]. If you omit [test_type], Internal is used. [test_type] can have the following values:

internal
Tests the SerDes. This is the default. The port must be in diagnostics mode to perform this test.

external
Tests both the SerDes and transceiver. The port must be in diagnostics mode to perform this test, and a loopback plug must be installed in the transceiver.

online
Tests communications between the port and its device node or device loop. The port being tested must be online and connected to a remote device. The port passes if the test frame that was sent by the ASIC matches the frame that is received. This test does not disrupt communication on the port.

cancel
Cancels the online test in progress.

status
Displays the status of a test in progress, or if there is no test in progress, the status of the test that was executed last.

Examples To run an internal or external port test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

```
admin start
```

2. Place the port in Diagnostics mode, enter the following command (*x* = port number) and press the Enter key.

```
set port x state diagnostics
```

3. Choose the type of port loopback test to run:

- To run an internal loopback test, enter the following:

  ```
  test port x internal
  ```

- To run an external loopback test, enter the following command. A loopback plug must be installed for this test to pass.

  ```
  test port x external
  ```

4. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload.
5. After the test type has been chosen and the command executed, a message on the screen will appear detailing the test results.
6. After the test is run, put the port back into online state by entering the following command (*x* = port number) and pressing the Enter key.

   ```
   set port x state online
   ```

7. To verify port is back online, enter the following command and press the Enter key. The contents of the AdminState field should display be “Online”.

   ```
   show port x
   ```

The online loopback (node-to-node) test requires that port be online and connected to a remote device. To run the online loopback test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

   ```
   admin start
   ```

2. To run the online loopback test, enter the following command and press the Enter key.

   ```
   test port x online
   ```

3. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload. Before running the test, make sure that the device attached to the port can handle the test parameters.

```
SANbox2 (admin) #> test port x online

A list of attributes with formatting and current values will
follow. Enter a new value or simply press the ENTER key to
accept the default value. If you wish to terminate this
process before reaching the end of the list press 'q' or 'Q'
and the ENTER key to do so.

  TestLength    (decimal value, 1-4294967295)   [100    ]
  FrameSize     (decimal value, 36-2148)        [256    ]
  DataPattern   (32-bit hex value or 'Default') [Default]
  StopOnError   (True/False)                    [False  ]
  Do you want to start the test? (y/n) [n]
```

4. After all parameter values are defined, press the Y key to start the test. After the command executes, a message on the screen will appear detailing the test results.

Uptime Command

Displays the elapsed up time since the switch was last reset and reset method. A hot reset or non-disruptive firmware activation does not reset the elapsed up time reported by this command.

Authority None

Syntax **uptime**

Examples The following is an example of the Uptime command:

```
SANbox2 #> uptime

  Elapsed up time  : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
  Reason last reset: NormalReset
```

User Command

Administers and displays user accounts.

Authority Admin account name and an Admin session. The Accounts and List keywords are available to all account names without an Admin session.

Syntax

user
accounts
add
delete [account_name]
edit
list

Keywords

accounts
Displays all user accounts that exist on the switch. This keyword is available to all account names without an Admin session.

add
Add a user account to the switch. You will be prompted for an account name, a password, authority, and an expiration date.

- A switch can have a maximum of 15 user accounts.
- Account names are limited to 15 characters; passwords must be 4–20 characters.
- Admin authority grants permission to use the Admin command to open an admin session, from which all commands can be entered. Without Admin authority, you are limited to view-only commands.
- The expiration date is expressed in the number of days until the account expires (2000 maximum). The switch will issue an expiration alarm every day for seven days prior to expiration. 0 (zero) specifies that the account has no expiration date.

delete [account_name]
Deletes the account name given by [account_name] from the switch.

edit
Initiates an edit session that prompts you for the account name for which to change the expiration date and authority.

list
Displays the list of users currently logged in and their session numbers. Provides the same function as the Show Users command. This keyword is available to all account names without an Admin session.

Notes User accounts are enforced in SANbox Manager only if the UserAuthentication parameter is set to True. The UserAuthentication default value is False. Refer to System keyword of the ”Set Setup Command” on page A-48 for information about setting the UserAuthentication parameter.

Examples

The following is an example of the User Accounts command:

```
SANbox2 (admin) #> user accounts

    Current list of user accounts
  ----------------------------
  images       (admin authority = False, never expires)
  admin        (admin authority = True , never expires)
  chuckca      (admin authority = False, expires in < 50 days)
  gregj        (admin authority = True , expires in < 100 days)
  fred         (admin authority = True , never expires)
```

The following is an example of the User Add command:

```
SANbox2 (admin) #> user add
    Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (4-20 chars)  : *******

please confirm account password: *******

set account expiration in days (0-2000, 0=never): [0] 100

should this account have admin authority? (y/n): [n] y

OK to add user account 'user1' with admin authority
and to expire in 100 days?

Please confirm (y/n): [n] y
```

The following is an example of the User Edit command:

```
SB211.192 (admin) #> user edit

      Press 'q' and the ENTER key to abort this command.

  account name (1-15 chars)      : user1
  set account expiration in days (0-2000, 0=never): [0]
  should this account have admin authority? (y/n): [n]

  OK to modify user account 'user1' with no admin authority
  and to expire in 0 days?

  Please confirm (y/n): [n]
```

The following is an example of the User Delete command:

```
SANbox2 (admin) #> user del user3

  The user account will be deleted.  Please confirm (y/n): [n] y
```

The following is an example of the User List command:

```
SANbox2 (admin) #> user list

    User                          Ethernet Addr-Port    Logged in Since
    ----                          ------------------    ---------------
  admin@OB-session1             10.20.68.108-1031     day month date time year
  admin@OB-session2             10.20.68.108-1034     day month date time year
  snmp@OB-session3              Unknown               day month date time year
  snmp@IB-session4              Unknown               day month date time year
  admin@OB-session5             Unknown               day month date time year
```

Whoami Command

Displays the account name, session number, and switch domain ID for the Telnet session.

Authority None

Syntax **whoami**

Examples The following is an example of the Whoami command:

```
SANbox2 #> whoami

User name       : admin@session2
Switch name     : SANbox2
Switch domain ID: 21 (0x15)
```

Zone Command

Manages zones and zone membership on a switch.

Authority Admin session and a Zoning Edit session. Refer to the "Zoning Command" on page A-90 for information about starting a Zoning Edit session. The List, Members, and Zonesets keywords are available without an Admin session.

Syntax

zone
add [zone] [member_list]
copy [zone_source] [zone_destination]
create [zone]
delete [zone]
list
members [zone]
remove [zone] [member_list]
rename [zone_old [zone_new]
type [zone] *[zone_type]*
zonesets [zone]

Keywords

add [zone] [member_list]
Specifies one or more ports/devices given by [members] to add to the zone named [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. A zone can have a maximum of 2000 members. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

The application verifies that the [members] format is correct, but does not validate that such a member exists.

copy [zone_source] [zone_destination]
Creates a new zone named [zone_destination] and copies the membership into it from the zone given by [zone_source].

create [zone]
Creates a zone with the name given by [zone]. An zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 1000 zones.

delete [zone]
Deletes the specified zone given by [zone] from the zoning database. If the zone is a component of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all zones and the zone sets of which they are components. This keyword does not require an Admin session.

members [zone]
Displays all members of the zone given by [zone]. This keyword does not require an Admin session.

remove [zone] [member_list]
Removes the ports/devices given by [member_list] from the zone given by [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

rename [zone_old] [zone_new]
Renames the zone given by [zone_old] to the zone given by [zone_new].

type [zone] ***[zone_type]***
Specifies the zone type given by [zone_type] to be assigned to the zone name given by [zone]. If you omit the [zone_type], the system displays the zone type for the zone given by [zone]. [zone_type] can be one of the following:

soft – name server zone

hardACL – Access control list hard zone. This keyword is case sensitive.

zonesets [zone]
Displays all zone sets of which the zone given by [zone] is a component. This keyword does not require an Admin session.

Examples

The following is an example of the Zone List command:

```
SANbox2 #> zone list

  Zone        ZoneSet
  ------------------
  wwn_b0241f
              zone_set_1

  wwn_23bd31
              zone_set_1

  wwn_221416
              zone_set_1

  wwn_2215c3
              zone_set_1

  wwn_0160ed
              zone_set_1

  wwn_c001b0
              zone_set_1

  wwn_401248
              zone_set_1

  wwn_02402f
              zone_set_1

  wwn_22412f
              zone_set_1
```

The following is an example of the Zone Members command:

```
SANbox2 #> zone members wwn_b0241f

  Current List of Members for Zone: wwn_b0241f
  --------------------------------
  50:06:04:82:bf:d2:18:c2
  50:06:04:82:bf:d2:18:d2
  21:00:00:e0:8b:02:41:2f
```

The following is an example of the Zone Zonesets command:

```
SANbox2 #> zone zonesets zone1

  Current List of ZoneSets for Zone: zone1
  ---------------------------------
  zone_set_1
```

Zoneset Command

Manages zone sets and component zones across the fabric.

Authority Admin session and a Zoning Edit session. Refer to the "Zoning Command" on page A-90 for information about starting a Zoning Edit session. The Active, List, and Zones keywords are available without an Admin session. You must close the Zoning Edit session before using the Activate and Deactivate keywords.

Syntax

zoneset
activate [zone_set]
active
add [zone_set] [zone_list]
copy [zone_set_source] [zone_set_destination]
create [zone_set]
deactivate
delete [zone_set]
list
remove [zone_set] [zone_list]
rename [zone_set_old] [zone_set_new]
zones [zone_set]

Keywords

activate [zone_set]
Activates the zone set given by [zone_set]. This keyword deactivates the active zone set. Close the Zoning Edit session before using this keyword.

active
Displays the name of the active zone set. This keyword does not require Admin session.

add [zone_set] [zone_list]
Adds a list of zones and aliases given by [zone_list] to the zone set given by [zone_set]. Use a <space> to delimit zone and alias names in [zone_list].

copy [zone_set_source] [zone_set_destination]
Creates a new zone set named [zone_set_destination] and copies into it the zones from the zone set given by [zone_set_source].

create [zone_set]
Creates the zone set with the name given by [zone_set]. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 zone sets.

deactivate
Deactivates the active zone set. Close the Zoning Edit session before using this keyword.

delete [zone_set]
Deletes the zone set given by [zone_set]. If the specified zone set is active, the command is suspended until the zone set is deactivated.

list
Displays a list of all zone sets. This keyword does not require an Admin session.

remove [zone_set] [zone_list]
Removes a list of zones given by [zone_list] from the zone set given by [zone_set]. Use a <space> to delimit zone names in [zone_list]. If [zone_set] is the active zone set, the zone will not be removed until the zone set has been deactivated.

rename [zone_set_old] [zone_set_new]
Renames the zone set given by [zone_set_old] to the name given by [zone_set_new]. You can rename the active zone set.

zones [zone_set]
Displays all zones that are components of the zone set given by [zone_set]. This keyword does not require an Admin session.

Notes

- A zone set must be active for its definitions to be applied to the fabric.
- Only one zone set can be active at one time.
- A zone can be a component of more than one zone set.

Examples

The following is an example of the Zoneset Active command:

```
SANbox2 #> zoneset active

  ActiveZoneSet    Bets
  LastActivatedBy  admin@OB-session6
  LastActivatedOn  day month date time year
```

The following is an example of the Zoneset List command:

```
SANbox2 #> zoneset list

  Current List of ZoneSets
  ------------------------
  alpha
  beta
```

The following is an example of the Zoneset Zones command:

```
SANbox2 #> zoneset zones ssss

  Current List of Zones for ZoneSet: ssss
  ---------------------------------
  zone1
  zone2
  zone3
```

Zoning Command

Opens a Zoning Edit session in which to create and manage zone sets and zones. Refer to the ”Zone Command” on page A-84 and the ”Zoneset Command” on page A-88.

Authority Admin session except for the Active, History, Limits, and List keywords.

Syntax

zoning
- active
- cancel
- clear
- edit
- history
- limits
- list
- restore
- save

Keywords

active
Displays information for the active zone set including component zones and zone members. This keyword does not require an Admin session.

cancel
Closes the current Zoning Edit session. Any unsaved changes are lost.

clear

Clears all inactive zone sets from the volatile edit copy of the zoning database. This keyword does not affect the non-volatile zoning database. However, if you enter the Zoning Clear command followed by the Zoning Save command, the non-volatile zoning database will be cleared from the switch.

Note: The preferred method for clearing the zoning database from the switch is the Reset Zoning command.

edit
Opens a Zoning Edit session.

history
Displays a history of zoning modifications. This keyword does not require an Admin session. History information includes the following:

- Time of the most recent zone set activation or deactivation and the user who performed it
- Time of the most recent modifications to the zoning database and the user who made them.
- Checksum for the zoning database

limits
Displays the number of zone sets, zones, aliases, members per zone, members per alias, and total members in the zoning database. This keyword also displays the switch zoning database limits, excluding the active zone set, which are described in Table A-16. This keyword does not require an Admin session.

Table A-16. Zoning Database Limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256)
MaxZones	Maximum number of zones (256)
MaxAliases	Maximum number of aliases (256).
MaxTotalMembers	Maximum number of zone and alias members (2000) that can be stored in the switch's zoning database.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (1000), excluding the orphan zone set, that can be stored in the switch's zoning database. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2000) that can be stored in the switch's zoning database.
MaxMembersPerAlias	Maximum number of members in all zones and aliases (2000)

list
Lists all fabric zoning definitions. This keyword does not require an Admin session.

restore
Reverts the changes to the zoning database that have been made during the current Zoning Edit session since the last Zoning Save command was entered.

save
Saves changes made during the current Zoning Edit session. The system will inform you that the zone set must be activated to implement any changes. This does not apply if you entered the Zoning Clear command during the Zoning Edit session.

Examples

The following is an example of the Zoning Edit command:

```
SANbox2 #> admin start


SANbox2 (admin) #> zoning edit
```

```
SANbox2 (admin-zoning) #>
.
.
SANbox2 (admin-zoning) #> zoning cancel

  Zoning edit mode will be canceled.  Please confirm (y/n): [n]   y

SANbox2 (admin) #> admin end
```

The following is an example of the Zoning Limits command:

```
SANbox2 #> zoning limits

  Zoning Attribute     Maximum   Current   [Name]
  ----------------     -------   -------   ------
  MaxZoneSets          256       6
  MaxZones             256       19
  MaxAliases           256       1
  MaxTotalMembers      2000      166
  MaxZonesInZoneSets   1000      19
  MaxMembersPerZone    2000
                                 10        D_1_JBOD_1
                                 23        D_1_Photons
                                 9         D_2_JBOD1
                                 16        D_2_NewJBOD_2
                                 5         E1JBOD1
                                 5         E2JBOD2
                                 3         LinkResetZone
                                 3         LinkResetZone2
                                 8         NewJBOD1
                                 8         NewJBOD2
                                 12        Q_1Photon1
                                 12        Q_2Photon2
                                 8         Q_1_NewJBOD1
                                 13        Q_1_Photon_1
                                 8         Q_2_NewJBOD2
                                 13        Q_2_Photon_2
                                 3         ZoneAlias
                                 3         ZoneDomainPort
                                 4         ZoneFCAddr
  MaxMembersPerAlias   2000
                                 2         AliasInAZone
```

The following is an example of the Zoning List command:

```
SANbox2 #> zoning list

  Active ZoneSet Information

  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f

              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31

              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16

              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3

  Configured Zoning Information

  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f

              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
```

```
wwn_221416
          50:06:04:82:bf:d2:18:c2
          50:06:04:82:bf:d2:18:d2
          10:00:00:00:c9:22:14:16

wwn_2215c3
          50:06:04:82:bf:d2:18:c2
          50:06:04:82:bf:d2:18:d2
          10:00:00:00:c9:22:15:
```

Appendix B
Graphing Port Performance

SANsurfer Fabric View application displays port performance using graphs. SANsurfer Fabric View plots data communication rates and total errors for selected ports as shown in Figure B-1. When graphing data communication rates, you can choose either frames/second or KB/second.

On the Solaris platform, if you launch the SANsurfer Fabric View application from the SANbox Manager application and SANsurfer Fabric View can not connect to the fabric, (for example, if you have reached the maximum number of SANbox Manager sessions on the entry switch), then SANsurfer Fabric View opens with a blue fabric icon displayed in the fabric tree.

Fabric status is displayed in text format after the fabric name in the fabric tree. The color of the icon indicates the current connection status as normal (green), warning (yellow), critical (red), or unmanageable (blue).

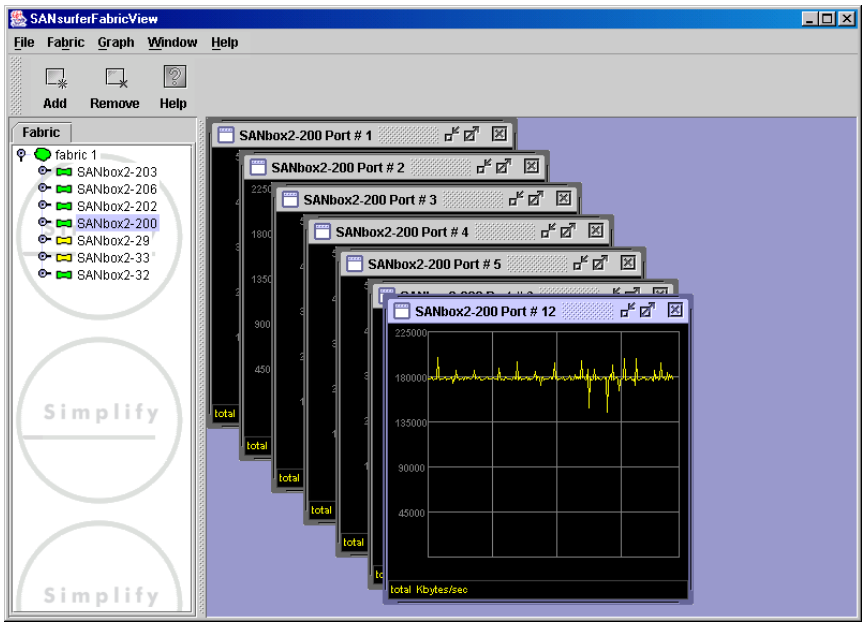


Figure B-1. Fabric View Graphs

This appendix describes how to do the following:

- Start SANsurfer Fabric View
- Exit SANsurfer Fabric View

- Save and Open SANsurfer Fabric View Default Fabric View Files
- Change the SANsurfer Fabric View Default Fabric File Password
- Set SANsurfer Fabric View preferences
- Set the polling frequency
- Display graphs
- Print graphs
- Rescale a selected graph
- Save graph statistics to a file

B.1 Starting SANsurfer Fabric View

To start SANsurfer Fabric View from within SANbox Manager, open the topology display and select **Start Fabric View** from the Fabric menu. When starting the SANsurfer Fabric View application from the SANbox Manager application on Linux and Solaris platforms, the fabric currently displayed in the SANbox Manager topology display opens automatically in the SANsurfer Fabric View topology display. On the Windows platform, you will need to manually open the fabric in the SANsurfer Fabric View topology display.

Note: On the Solaris platform, if you launch the SANsurfer Fabric View application from the SANbox Manager application and SANsurfer Fabric View can not connect to the fabric, (for example, if you have reached the maximum number of SANbox Manager sessions on the entry switch), then SANsurfer Fabric View opens with a blue fabric icon displayed in the fabric tree. The reason for status displayed after the fabric name in the fabric tree will indicate the reason for failure to connect.

B.2 Exiting SANsurfer Fabric View

To exit a SANsurfer Fabric View session, open the File menu and select **Exit**. The current fabric view is automatically saved to your default fabric view file upon exit, if you have defined an encryption key. The key is encrypted and saved with your default fabric view file. A fabric view file contains the set of fabrics that have been added and the graphs that have been opened during a SANsurfer Fabric View session. If you have not yet defined an encryption key, the Save Default Fabric View File dialog, shown in Figure B-2, prompts you to save the current fabric view as the default fabric view file. Refer to ”Changing the Default Fabric View File Encryption Key” on page B-4 for information about defining and changing this encryption key.

In the Save Default Fabric View File dialog, enter an encryption key in the Default Fabric File Encryption Key field. Re-enter the encryption key in the Re-enter Encryption Key to Confirm field. Click the **OK** button to save the current set of SANsurfer Fabric View fabrics to the default fabric view file in the working directory.

To prevent SANsurfer Fabric View from prompting you to save the default fabric view file between sessions, set the Auto Load and Save Graphing Environment setting to Enable (default). Refer to "Setting SANsurfer Fabric View Preferences" on page B-4 for more information.

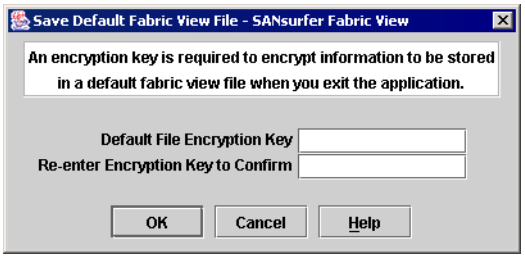

Save Default Fabric View File - SANsurfer Fabric View
An encryption key is required to encrypt information to be stored in a default fabric view file when you exit the application.
Default File Encryption Key
Re-enter Encryption Key to Confirm
OK
Cancel
Help

Figure B-2. Save Default Fabric View File Dialog – SANsurfer Fabric View

In your next SANsurfer Fabric View session, the Load Default Fabric File dialog shown in Figure B-3 prompts you to load the default fabric view file and to specify its encryption key, if there is one. In the Default Fabric File Encryption Key field, enter the encryption key and click the **Load View File** button. If you do not want to load the default fabric view file, click the **Continue Without Loading** button to open the SANsurfer Fabric View with no fabric displayed.

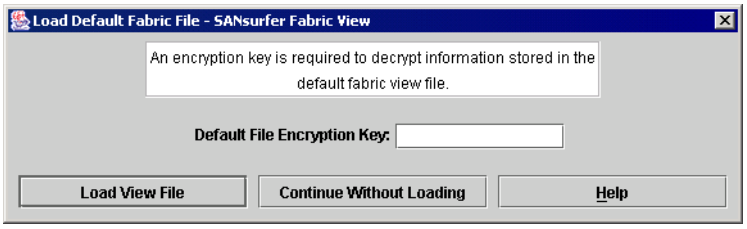

Load Default Fabric File - SANsurfer Fabric View
An encryption key is required to decrypt information stored in the default fabric view file.
Default File Encryption Key:
Load View File
Continue Without Loading
Help

Figure B-3. Load Default Fabric File Dialog – SANsurfer Fabric View

B.3 Saving and Opening Fabric View Files

In addition to the SANsurfer Fabric View default fabric view file, you can save and open your own fabric view files. The fabric view file contains the set of fabrics, graphs, and graphing options. To save a fabric view file, do the following:

1. Open the File menu and select **Save View As** to open the Save View dialog.
2. Enter a name for the fabric file or click the **Browse** button to select an existing file. Files are saved in the working directory.
3. Enter a password. When you attempt to open this fabric file, you will be prompted for this password. If you leave the File Password field blank, no password is required.

To open a fabric view file, do the following:

1. Open the File menu and select **Open View File** to open the Open View dialog.
2. Enter a name for the fabric file or click the **Browse** button to select an existing file.

B.4 Changing the Default Fabric View File Encryption Key

To change the encryption key for the default fabric view file, do the following:

1. Open the File menu and select **Save Default File Fabric View File** to open the Save Default File Fabric View File dialog.
2. Enter the new password in the Default File Encryption Key field.
3. Re-enter the same password in the Re-enter Encryption Key to Confirm field.
4. Click the **OK** button to save the changes.

B.5 Setting SANsurfer Fabric View Preferences

To set preferences, open the File menu and select **Preferences** to open the Preferences dialog shown in Figure B-4. Set the following preferences and click the **OK** button to save the changes:

- Change the location of the working directory in which to save files
- Change the location of the browser used to view the online help.
- Enable or disable the **Auto Load and Auto Save Graphing Options** preference. When enabled, SANsurfer Fabric View prompts you to save and load the default fabric file between sessions. Refer to ”Exiting SANsurfer Fabric View” on page B-2 for more information on the default fabric view file.

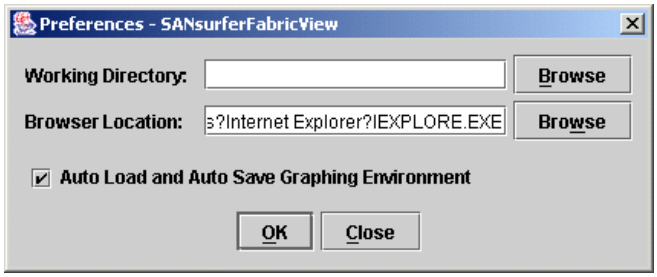


Figure B-4. Preferences – SANsurfer Fabric View

B.6 Setting the Polling Frequency

Fabric View updates the graphs once per second by default. To change this polling frequency, do the following:

1. Open the Graph menu, and select **Set Polling Frequency** to open the Set Graph Polling Frequency dialog.
2. Enter the new polling interval in seconds [1–60]. Fabric View will update the graphs once during the interval. For example, setting the polling frequency to 5 seconds will return 1 second's worth of data every 5 seconds.
3. Click the **OK** button to save the changes.

B.7 Displaying Graphs

To display graphs, do the following:

1. Open the Fabric menu and select **Add Fabric** or click the **Add** button. Enter a fabric name and an IP address in the Add a New Fabric dialog. Include an account name and a password if required.
2. Set the graphing options and polling frequency. By default, SANsurfer Fabric View plots total bytes transmitted and received at a polling frequency of once per second. Refer to "Customizing Graphs" on page B-6 for information about changing what is plotted and how it is plotted.
3. You can display graphs in the following ways:
   - Click on a switch entry handle and select one or more ports.
   - Right click on a switch icon in the fabric tree and select **Open Graph for All Ports on Switch** or **Open Graph for All Logged-In Ports on Switch** from the pull-down menu.
4. You can move graphs around individually by clicking and dragging, or you can arrange them as a group. Refer to "Arranging Graphs in the Display" on page B-6 for more information.

To remove a graph, click the graph **Remove** button. To remove all graphs, open the Window menu and select **Close All**.

To remove a fabric and its graphs, select the fabric in the fabric tree, then select **Remove Fabric** from the Fabric menu. You can also right click on a fabric and select **Remove Fabric** for the popup menu.

Right clicking on a graph opens a popup menu from which you can change graph options, print a graph, or save the graph statistics to a file.

B.7.1
Arranging Graphs in the Display

To arrange and size graphs in the display, open the Window menu and select **Cascade**, **Tile**, or **Close All**.

- **Cascade** overlaps the graphs so that all graphs are at least partially visible.
- **Tile** arranges the graphs in non-overlapping rows and columns.
- **Close All** closes all graphs.

You can also click a graph on the Window menu to bring that graph to the front.

B.7.2
Customizing Graphs

You can customize the graph polling frequency, what is plotted in the graphs, and the graph color scheme. To set the polling frequency for all graphs, open the Graph menu and select **Set Polling Frequency...**. Enter an interval in seconds (0–60) in the dialog box and click the **OK** button.

To choose what is to be plotted, open the Graph menu and select **Modify Graph Options...**. You can also right click on a graph and select **Change Graph Options**. This opens the Default Graph Options dialog shown in Figure B-5.

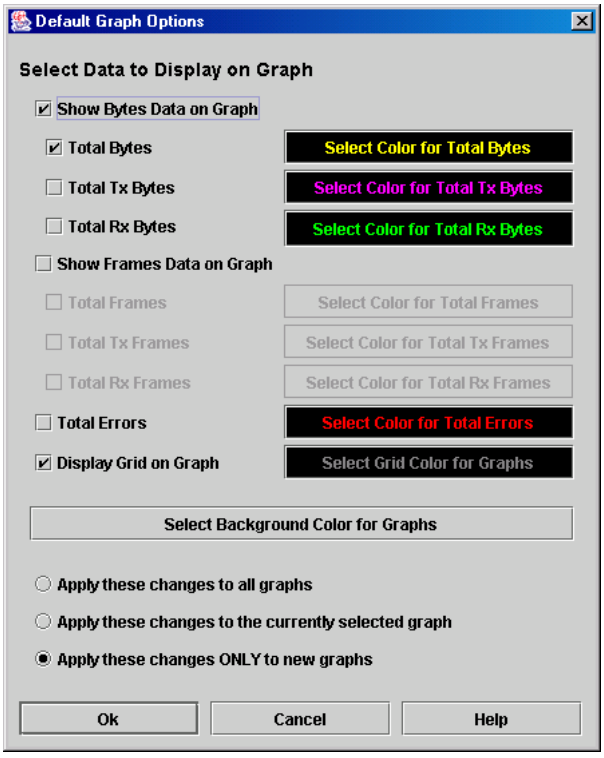

Default Graph Options
Select Data to Display on Graph
Show Bytes Data on Graph
Total Bytes
Select Color for Total Bytes
Total Tx Bytes
Select Color for Total Tx Bytes
Total Rx Bytes
Select Color for Total Rx Bytes
Show Frames Data on Graph
Total Frames
Select Color for Total Frames
Total Tx Frames
Select Color for Total Tx Frames
Total Rx Frames
Select Color for Total Rx Frames
Total Errors
Select Color for Total Errors
Display Grid on Graph
Select Grid Color for Graphs
Select Background Color for Graphs
Apply these changes to all graphs
Apply these changes to the currently selected graph
Apply these changes ONLY to new graphs
Ok
Cancel
Help

Figure B-5. Default Graph Options Dialog

To modify the graph options, do the following:

1. Choose the units for the graph:
   - Select the **Show Bytes Data on Graph** check box to plot data in KBytes/second
   - Select the **Show Frames Data on Graph** check box to plot data in frames/second.
2. Choose what data type to plot. For example, if you selected **Show Frames Data on Graph** in step 1, you can plot one or all of the following:
   - Total frames transmitted and received (**Total Frames**)
   - Total frames transmitted (**Total Tx Frames**)
   - Total frames received (**Total Rx Frames**)

   In addition to these, you can also plot total errors by selecting the **Total Errors** check box.
3. Display or hide the unit grid. Select the **Display Grid on Graph** check box to display the unit grid.

4. Choose the color scheme for the graph. Click a Select Color button to open its corresponding Select Color dialog, which allows you to select a new color scheme. You can select the color for each data type, the unit grid, and the background by clicking the corresponding color field or button. In each case, you can choose a color using the Swatches, Red-Green-Blue (RGB), or Hue-Saturation-Brightness (HSB) method.

   Note: Clicking the **Reset** button in the Swatches, HSB, and RGB tab pages of the Select Color dialogs will reset the colors in the Preview area to the last saved color scheme. At this point you are only selecting a new color scheme to be saved.

   - Swatches – Click the **Swatches** tab. Select a swatch from the palette.
   - HSB – Click the **HSB** tab. Select a color using any of the following methods:
     - Click in the color palette.
     - Select the **H**, **S**, or **B** button and use the slide to vary the selected value.
     - Enter values in the H, S, or B input fields.
   - RGB – Click the **RGB** tab. Select a color by moving the slides to adjust the values for red, blue, and green; or enter values in the input fields.
5. In the Default Graph Options dialog, click the corresponding radio button to apply changes to all graphs, the currently selected graph, or all new graphs.
6. In the Default Graph Options dialog, click the **OK** button to save the color scheme changes and close the dialog.

B.8 Printing Graphs

To print a graph, select a graph, then open the File menu and select **Print Graph Window**. You can also right click on a graph and select **Print Graph Window** from the popup menu.

B.9 Rescaling a Selected Graph

The Rescale Selected Graph option auto-scales downward and re-positions the data within a graphic window to display all new data captured by the graph. To rescale a selected graph, do the following:

1. Select a displayed graph.
2. Open the Graph menu and select **Rescale Selected Graph**, or right-click on the graph and select **Rescale** from the popup menu.
3. View the data in the graph window.
4. Click the **Save** button.

B.10 Saving Graph Statistics to a File

Statistics for one or all graphs can be saved to a file that can be opened with a spreadsheet application. To save a graph statistics file, do the following:

1. Select a graph.
2. Open the File menu, and select **Save Current Graph Statistics to a File** to save the selected graph or select **Save All Graph Statistics to a File**. You can also right click on a graph and select **Save Statistics to File**.
3. In the Save dialog, enter a path name for the file. By default, the file is saved in the working directory.
4. Click the **Save** button.

Notes

Appendix C
Messages

This appendix lists the SANbox Manager messages by task, dialog, or display. To find a message and what to do about it, consider what task you are performing, and refer to the corresponding subsection.

- ”Fabrics File—Open, Save” on page C-1
- ”Add a Fabric” on page C-2
- ”Network Properties Dialog” on page C-3
- ”Switch Properties Dialog” on page C-4
- ”Port Properties Dialog” on page C-8
- ”Faceplate Display” on page C-10
- ”Load Firmware Dialog” on page C-13
- ”Firmware Fallback Dialog” on page C-13
- ”Port Loopback Test Dialog” on page C-15
- ”Extended Credits Wizard” on page C-17
- ”Zoning Dialog” on page C-17
- ”Restore Configuration Dialog” on page C-20
- ”Save Fabric View” on page C-20
- ”Trap Configuration Dialog” on page C-21

C.1 Fabrics File—Open, Save

Table C-1. Fabrics File – Open, Save Messages

Message	User Action
Failed opening fabrics list file *filename*.	Verify that the specified file exists on a file system that is reachable, and that the user has permissions to read the file.
Failed saving fabrics list file *filename*.	Verify that the specified file system is reachable, and that the user has permissions to write to the file system, to the directory, and to the file.

C.2 Add a Fabric

Table C-2. Add a Fabric Messages

Message	User Action
Fabric *fabricname* already exists! *Or* Fabric name already in use.	Specify a name for the fabric that is not already assigned to an existing fabric.
Invalid IP Address	Verify that the IP address specified is syntactically correctly.
The entry switch is of a type that is not supported.	The switch hardware or firmware version of the switch at the specified IP address is not supported. Choose the IP address of a different switch, or update the firmware using Telnet or the appropriate version of the application.
The maximum number of management sessions on the entry switch has been exceeded.	The application cannot establish a session with the fabric because too many sessions are already open. Close any other application or Telnet sessions to the fabric and try again.
Unable to login to switch. Reason: …	Verify that the user name and password entered in the dialog box are valid login information for an account on the switch specified by the IP address field.
Unknown host *hostname*.	Verify that the host name specified for the IP address is a valid hostname for a switch in the fabric, and that the switch is reachable from the user's workstation.
Verify correct user name and password and retry.	Either the user name or password is incorrect. Enter the correct values and retry.

C.3 Network Properties Dialog

Table C-3. Network Properties Dialog Messages

Message	User Action
Attempt to change snmp community strings failed. *Or* Attempt to change syslog configuration failed.	Verify that the data is valid, that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.
Unable to apply invalid syslog host address	Verify that either a syntactically correct IP address was specified for the syslog host, or that a host name was specified for a valid syslog host that is reachable from the user's workstation.

C.4 Switch Properties Dialog

Table C-4. Switch Properties Dialog Messages

Message	User Action
Attempt to change chassis name failed Or Attempt to set ISL security failed. Or Attempt to set in-band management failed. Or Attempt to change domain ID lock failed. Or Attempt to change SNMP configuration failed Or Attempt to change IP configuration failed Or Attempt to change chassis configuration failed Or Attempt to change timeout values failed Or Attempt to change broadcast support failed	Verify that the data is valid, that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.
Changing the domain ID may cause the SANbox 1Gb switches to isolate from the fabric. Do you still want to make this change?	Verify that all information is valid and retry the configuration change. Consult the documentation for valid configurations. Valid domain IDs must be in the range 1 to 239, and must be unique within a fabric. If the fabric contains SANbox with E_Port switches, then all domain IDs must be in the same range of sixteen values: 1…16, 17…32, and so on.
Disabling in-band management will make the switch unreachable. Do you wish to continue with this change?	If this feature is disabled, this switch will no longer be manageable through this session to the fabric. If this is acceptable, then continue; otherwise cancel the operation.

Table C-4. Switch Properties Dialog Messages (Continued)

Message	User Action
Duplicate domain ID specified.	Verify that all information is valid and retry the configuration change. Consult the documentation for valid configurations. Valid domain IDs must be in the range 1 to 239, and must be unique within a fabric. If the fabric contains SANbox with E_Port switches, then all domain IDs must be in the same range of sixteen values: 1…16, 17…32, and so on.
If you set this inband switch offline you will need an ethernet connection to the switch to put it back online. Do you want to set switch offline? Or If you set this inband switch in diagnostics mode you will need an ethernet connection to the switch to put it back online. Do you want to set switch in diagnostics mode?	These changes will prevent the application from communicating with the switch in the fabric. Before applying the changes, verify that the switch is reachable through its own Ethernet port, then add a new fabric (Fabric>Add Fabric) at the switch's own IP address.
IP configuration changes will not take effect until switch is reset.	The new IP configuration has been set on the switch, but the user has decided not to reset the switch at this time. Arrange a time when it is acceptable to disrupt communications between the hosts and storage systems, then reset the switch to make the changes effective.
Modification of IP configuration will require a switch reset to take effect. The reset may disrupt traffic. Do you wish to continue?	This configuration information will not become effective unless the switch is reset. Resetting a switch in the fabric will cause the servers and storage systems attached to the fabric to lose communications until the switch reset is complete and the fabric has re-initialized. If this is acceptable, then continue; otherwise cancel the reset operation.

Table C-4. Switch Properties Dialog Messages (Continued)

Message	User Action
Out of range domain ID specified.	Verify that all information is valid and retry the configuration change. Consult the documentation for valid configurations. Valid domain IDs must be in the range 1 to 239, and must be unique within a fabric. If the fabric contains SANbox with E_Port switches, then all domain IDs must be in the same range of sixteen values: 1…16, 17…32, and so on.
Received error in attempting to edit switch configuration. Or Received error in attempting to save switch configuration. Or Received error in attempting to activate switch configuration.	Verify that the data is valid, that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.
Reset will complete shortly. There will be a brief loss of connectivity with switch.	Wait for the switch to become reachable again. This may take up to one minute.
The new domain ID specified is invalid. Unable to apply invalid chassis/fabric ID values	Verify that all information is valid and retry the configuration change. Consult the documentation for valid configurations. Valid domain IDs must be in the range 1 to 239, and must be unique within a fabric. If the fabric contains SANbox with E_Port switches, then all domain IDs must be in the same range of sixteen values: 1…16, 17…32, and so on.

Table C-4. Switch Properties Dialog Messages (Continued)

Message	User Action
Unable to apply changes. Failed to obtain admin privileges.	Verify that another user is not currently modifying the switch configuration, using either the management application, or a telnet login, or any application.
Unable to apply invalid timeout values Or Unable to apply invalid IP address Or Unable to apply invalid trap address Or Unable to apply invalid subnet mask Or Unable to apply invalid gateway address Or Unable to apply invalid ARP timeout value	Verify that all information is valid and retry the configuration change. Consult the documentation for valid configurations. Valid domain IDs must be in the range 1 to 239, and must be unique within a fabric. If the fabric contains SANbox with E_Port switches, then all domain IDs must be in the same range of sixteen values: 1…16, 17…32, and so on.

C.5 Port Properties Dialog

Table C-5. Port Properties Dialog Messages

Message	User Action
Invalid value entered for interop credits. Or Failed to set I/O stream guard change. Or Failed to set new interop credits. Or Request to save and activate config failed. Or Received error in attempting to edit switch configuration. Or Received error in attempting to save switch configuration. Or Received error in attempting to activate switch configuration.	Verify that the data is valid, that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.
Received error in attempting to release admin privileges	The application did not receive a required response from the switch. This may be caused by a momentary or extended loss of communications with the fabric. First refresh the information in the display to determine whether the changes took effect. If not, retry the changes. If the error persists, determine whether communications with the switch have stopped, and resolve any network problems. When communication with the fabric has resumed, return to the application to view the properties for the port and verify whether the changes took effect. If not, then retry the changes.
Request to save and activate config failed.	Verify that the data is valid, that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.

Table C-5. Port Properties Dialog Messages (Continued)

Message	User Action
Unable to apply changes. Failed to obtain admin privileges.	Verify that another user is not currently modifying the switch configuration, using either the management application, or a Telnet login, or any other application, and then retry the operation.
Unable to confirm that port changes were successful.	The application did not receive a required response from the switch. This may be caused by a momentary or extended loss of communications with the fabric. First refresh the information in the display to determine whether the changes took effect. If not, retry the changes. If the error persists, determine whether communications with the switch have stopped, and resolve any network problems. When communication with the fabric has resumed, return to the application to view the properties for the port and verify whether the changes took effect. If not, then retry the changes.
Unable to successfully apply port speed change. Or Unable to successfully apply port state change. Or Unable to successfully apply port type change.	Verify that the data is valid, that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.

C.6 Faceplate Display

Table C-6. Faceplate Display Messages

Message	User Action
Failed to clear the trap log.	Verify that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.
Necessary information is missing for this switch. Firmware version on this switch is unsupported.	The user has attempted an action which cannot be completed because it requires information from the switch which the switch does not support. Update the firmware on the switch to the latest version.
Necessary information is missing for this switch. Retry later.	The user has attempted an action which cannot be completed until specific information has been retrieved from the switch. This condition usually corrects within several seconds. If the condition doesn't correct itself, verify that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation. When the switch is reachable again, then wait for the application to retrieve complete information from the switch (this may take up to one minute), or refresh the display.
One of the selected ports is currently in use as a donor port to allow for extended credits on another port. Modifications to donor ports are not permitted.	Unselect the donor ports, and then retry the operation.
Port reset failed Or Request to reset to factory defaults has failed. Or Request for switch reset failed	Verify that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.

Table C-6. Faceplate Display Messages (Continued)

Message	User Action
Request for switch reset failed because admin access was not available.	Verify that another user is not currently modifying the switch configuration, using either the management application, or a telnet login, or any application, and then retry the operation.
Reset will complete shortly. There will be a brief loss of connectivity with switch.	Wait for the switch to become reachable again. This may take up to one minute.
Resetting the switch will disrupt traffic. Do you wish to continue? *Or* Deactivating the active zone set will disrupt traffic. Do you wish to continue?	The requested action will cause the servers and storage systems attached to the fabric to lose communications until the switch reset is complete and the fabric has re-initialized. If this is acceptable, then continue; otherwise cancel the operation.
Resetting to factory defaults will disrupt traffic and cause current switch configuration to be lost.	This action is disruptive to the fabric. Verify that this is the action that you wish to take.
Showing Last Known State	The switch state displayed by the application cannot be updated because the switch has become unreachable. Verify that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation.
The file currently exists.	The selected switch archive file already exists. If it is acceptable to overwrite the file, then continue. Otherwise, return and select a different archive file.
The online port loopback test can only be performed on a single port at a time. There are multiple ports selected. Continue with loopback test on first selected port	Select only a single port, and then retry the operation.

Table C-6. Faceplate Display Messages (Continued)

Message	User Action
The zoning information you are about to edit is incomplete. If you apply changes you will possibly lose zoning information.	The application has not been able to completely read the current zoning database from the switch. If the user edits the incomplete database information and applies the changes, then any information which has not been read from the switch will be lost. If this is acceptable, then continue. Otherwise, verify that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation then refresh the display and verify that the zoning database has been completely read, then retry the operation.
Unable to perform request. Switch is currently unreachable.	Verify that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the operation.
You can not perform this operation in-band.	Isolate the switch from the fabric, connect directly to the Ethernet port, and retry the operation.
Zone set deactivation failed.	Verify that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.

C.7 Firmware Fallback Dialog

Table C-7. Firmware Fallback Dialog Messages

Message	User Action
Attempt to revert to fallback firmware failed	The switch was unable to fall back to the previous firmware. Correct the problem specified and retry the operation.
Request to get admin privileges failed.	Verify that another user is not currently modifying the switch configuration, using either the management application, or a Telnet login, or any application, and then retry the operation.
Switch must be reset to activate fallback firmware. A reset will disrupt traffic. Reset now?	The firmware will not begin executing the fallback version until the next time the switch is reset. The user may reset the switch now, but resetting the switch is disruptive to the fabric. If this is acceptable, then continue. Otherwise, schedule an appropriate time during maintenance to reset the switch.

C.8 Load Firmware Dialog

Table C-8. Load Firmware Dialog Messages

Message	User Action
Bad checksum/CRC for the firmware image or incorrect firmware image for this type of switch.	Select the correct firmware file for this switch.
File was not found.	Verify that the firmware file specified actually exists, or specify a new firmware file.
Firmware image had a bad CRC or was invalid for this type of switch.	Select a valid firmware image for this type of switch and retry the operation.

Table C-8. Load Firmware Dialog Messages (Continued)

Message	User Action
Firmware upload complete. The switch must be reset to activate new firmware. Reset now?	The new firmware will not be executed until the switch is reset. Resetting a switch in the fabric will cause the servers and storage systems attached to the fabric to lose communications until the switch reset is complete and the fabric has reinitialized. If this is acceptable, then continue; otherwise cancel the reset operation.
Firmware upload status unknown. Image has been uploaded, but confirmation from the switch was not received.	The application lost communications with the switch while the switch was unpacking the firmware image. If the problem was temporary, examine the firmware versions on the switch to verify that the firmware was unpacked correctly, or upload a new firmware image to the switch.
The flash memory on the switch may be too small for this image.	Select an appropriate firmware image for this type of switch and retry the operation.
Unable to load firmware.	An unspecified error has occurred. Verify that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the firmware upload.
Unable to read file.	Verify that the firmware file specified exists and is readable by the user, on a file system readable by the user, or specify a new firmware file.

C.9 Port Loopback Test Dialog

Table C-9. Port Loopback Test Dialog Messages

Message	User Action
Attempt to put port in diagnostic state has failed. Unable to continue with port test.	Verify that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.
External port test requires a loopback device be plugged into the selected port. Click "OK" when loopback device is installed.	Verify that a loopback device is attached to the port before starting loopback test.
Failed to correctly restore port states for one or more ports.	Return to the faceplate view and select View>Port State to determine which port was not restored to its original state. Select the port, and then select Port>Port Properties to restore the port state.
Invalid frame count value. Or Invalid frame size. Must be 36 to 2148. Or Invalid hex pattern. Up to 8 hex digits allowed.	Verify that all information is valid and retry the loopback test.
No device detected in selected port yet. Test will not be run on empty port.	Verify that a loopback device is attached to the port before starting loopback test. Verify that the port is online with an active login before starting the loopback test.
Request to get admin privileges failed.	Verify that another user is not currently modifying the switch configuration, using either the management application, or a telnet login, or any application, and then retry the operation.
Request to start loopback test failed. Or Request to stop loopback test failed. Or Request for loopback test results failed Or Request to reset loopback test results failed.	Verify that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration change.

Table C-9. Port Loopback Test Dialog Messages (Continued)

Message	User Action
Switch is currently unreachable. Unable to accurately report status of port test.	The application lost communications with the switch while the switch was running the loopback tests, and could not determine whether the tests completed. If the problem was temporary, restart the loopback tests.
The port selected for online port test must be online with active login.	Verify that the port is online with an active login before starting the loopback test.
Timed out on response notifications. Test terminated.	The application lost communications with the switch while the switch was running the loopback tests, and could not determine whether the tests completed. If the problem was temporary, restart the loopback tests.
Unable to perform loopback test on port... ■ because port is not in diagnostic state. ■ because port is a donor port. ■ because there is already a port test in progress.	Correct the error indicated, and retry the loopback test.

C.10 Extended Credits Wizard

Table C-10. Extended Credits Wizard Messages

Message	User Action
Request for admin failed.	Verify that another user is not currently modifying the switch configuration, using either the management application, or a telnet login, or any application, and then retry the operation.
Request for extended credits failed	Verify that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the operation.
Request to edit config failed. Or Request to save and activate config failed.	Verify that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the operation.

C.11 Zoning Dialog

Table C-11. Zoning Dialog Messages

Message	User Action
Error loading zoning	Verify that the specified zoning configuration file exists on a file system that is reachable, and that the user has permissions to read the file.
Error returned from switch	Verify that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then refresh the zoning information from the switch to determine whether any of the zoning configuration has been applied. If necessary, re-edit the zoning configuration and apply to the switch again.

Table C-11. Zoning Dialog Messages (Continued)

Message	User Action
Error saving zoning	Verify that the specified zoning configuration file exists on a file system that is reachable, and that the user has permissions to write the file.
Failed to obtain admin privileges	Verify that another user is not currently modifying the switch configuration, using either the management application, or a telnet login, or any application, and then retry the operation.
Invalid name. Valid names start with a letter and valid chars include: ■ all alphanumeric chars [aA - zZ] [0 - 9] ■ symbols ['$', '_', and '-'	Select a valid name for the object and retry the operation.
Maximum number of zones created.	Remove unnecessary objects from the zoning configuration and retry the operation.
No member(s) selected; nothing to add.	Select the members to add, then retry the operation.
No response from the switch. Or Saving zoning data failed	Verify that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then refresh the zoning information from the switch to determine whether any of the zoning configuration has been applied. If necessary, re-edit the zoning configuration and apply to the switch again.
The maximum number of members has been reached. Or The maximum number of members per zone has been reached	Remove unnecessary objects from the zoning configuration and retry the operation.
The orphan set is a place a holder for zones that are not in a set. It can not be deleted.	Do not attempt to delete the orphan zone set.

Table C-11. Zoning Dialog Messages (Continued)

Message	User Action
The zone set you attempting to activate contains port based zoning and there are switches in the fabric that might not support this type of zoning. Some E_Ports may isolate. Do you wish to continue?	Not all switch vendors support port-based zoning. Consult the manual for these vendors' switches to determine whether to apply this zoning configuration to the fabric.
The zoning configuration has been changed. Would you like to apply your changes?	The zoning configuration includes changes that have not been applied to the switch. Select Yes to apply the changes to the switch before continuing, or select No to discard the changes and continue.
There is already a zone by that name in a different Zone set. Would you like to add that zone to this Zone Set?	If the existing zone is the same as zone that the user wants to add to this zoneset, then continue. Otherwise, select a unique name for the new zone and retry the operation.
There is already a zone set with that name. Or There is already a zone with that name. Or There is already a alias with that name.	Select a unique name for the new object and retry the operation.
This zoning configuration exceeds the limits for this switch.	Remove unnecessary objects from the zoning configuration and retry the operation.
Unable to create alias.	The zoning configuration already contains the maximum allowed zoning aliases. Delete any unwanted aliases and retry the operation.
You are about to save a zoning configuration that was not completely read in. Saving this version will make the incomplete database permanent.	An error was encountered while reading the zoning database from the switch, and so the database edited by the user may be missing some zoning information.
You have zones in the orphan zone set. These are not saved in the switch. Would you like to continue?	Orphan zones are not applied to the switch. If the orphan zones are to be applied to the switch, they must first be added to a configured zoneset. Orphan set is not saved on switches, and is used only in the application while configuring zoning information.

C.12 Restore Configuration Dialog

Table C-12. Restore Configuration Dialog Messages

Message	User Action
Failed parsing *filename*	Verify that the file specified is a valid archive file, and retry the operation.
Possibly failed check switch!	The application lost communications with the switch while restoring the archived configuration, and could not determine whether the operation completed. If the problem was temporary, retry the operation.
Restore failed!	Verify that the user has permissions to modify the configuration on the switch, that the switch is reachable in the fabric, and that the fabric is reachable from the user's workstation, then retry the configuration restore.

C.13 Save Fabric View

Table C-13. Save Fabric View Messages

Message	User Action
File "filename" already exists. Do you want to overwrite?	The specified view file already exists. Cancel, or continue to overwrite the file.

C.14 Trap Configuration Dialog

Table C-14. Trap Configuration Dialog Messages

Message	User Action
Invalid rising threshold Or Invalid falling threshold Or Invalid sample interval.	Verify that the information is correct and then retry.
You must wait for trap information to be read first. Or You must wait for alarm threshold information to be read first.	The application has not completely read in some configuration information which is needed for this operation. Wait until the information has been completely read and then retry.

Notes

Glossary

Access Control List Zone

Access Control List zoning divides the fabric for purposes of controlling discovery and inbound traffic.

Active Zone Set

The zone set that defines the current zoning for the fabric.

Active Firmware

The firmware image on the switch that is in use.

Activity LED

A port LED that indicates when frames are entering or leaving the port.

Administrative State

State that determines the operating state of the port, I/O blade, or switch. The configured administrative state is stored in the switch configuration. The configured administrative state can be temporarily overridden using the command line interface.

Alarm

A message generated by the switch that specifically requests attention. Alarms are generated by several switch processes. Some alarms can be configured.

Alias

A named set of ports or devices. An alias is not a zone, and can not have a zone or another alias as a member.

AL_PA

Arbitrated Loop Physical Address

Arbitrated Loop

A Fibre Channel topology where ports use arbitration to establish a point-to-point circuit.

Arbitrated Loop Physical Address (AL_PA)

A unique one-byte value assigned during loop initialization to each NL_Port on a loop.

ASIC

Application Specific Integrated Circuit

Auto Save

Zoning parameter that determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to permanent memory on that switch.

BootP

A type of network server.

Buffer Credit

A measure of port buffer capacity equal to one frame.

Cascade Topology

A fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology.

Class 2 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports wit h acknowledgment provided.

Class 3 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment.

Configured Zone Sets

The zone sets stored on a switch excluding the active zone set.

Default Visibility

Zoning parameter that determines the level of communication among ports/devices when there is no active zone set.

Domain ID

User defined number that identifies the switch in the fabric.

Event Log

Log of messages describing events that occur in the fabric.

Expansion Port

E_Port that connects to another FC-SW-2 compliant switch.

Fabric Database

The set of fabrics that have been opened during a SANbox Manager session.

Fabric Management Switch

The switch through which the fabric is managed.

Fabric Name

User defined name associated with the file that contains user list data for the fabric.

Fabric Port

An F_Port.

Fabric View File

A file containing a set of fabrics that were opened and saved during a previous SANbox Manager session.

Fan Fail LED

An LED that indicates that a cooling fan in the switch is operating below standard.

FC-PLDA

Fibre Channel Private Loop Direct Attach

Flash Memory

Memory on the switch that contains the chassis control firmware.

Force PROM Mode

See Maintenance Mode.

Frame

Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter.

FRU

Field Replaceable Unit

Heartbeat LED

A chassis LED that indicates the status of the internal switch processor and the results of the Power-On Self-Test.

Inactive Firmware

The firmware image on the switch that is not in use.

In-band Management

The ability to manage a switch through another switch over an inter-switch link.

Initiator

The device that initiates a data exchange with a target device.

In-Order-Delivery

A feature that requires that frames be received in the same order in which they were sent.

Input Power LED

A chassis LED that indicates that the switch logic circuitry is receiving proper DC voltages.

Inter-Switch Link

The connection between two switches using E_Ports.

IP

Internet Protocol

LIP

Loop Initialization Primitive sequence

Logged-In LED

A port LED on SANbox2-8c and SANbox2-16 switches that indicates device login or loop initialization status.

Maintenance Button

Formerly known as the Force PROM button. Momentary button on the switch used to reset the switch or place the switch in maintenance mode.

Maintenance Mode

Formerly known as force PROM mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes.

Management Information Base

A set of guidelines and definitions for SNMP functions.

Management Workstation

PC workstation that manages the fabric through the fabric management switch.

Mesh Topology

A fabric in which each chassis has at least one port directly connected to each other chassis in the fabric.

MIB

Management Information Base

Multistage Topology

A fabric in which two or more edge switches connect to one or more core switches.

NL_Port

Node Loop Port. A Fibre Channel device port that supports arbitrated loop protocol.

N_Port

Node Port. A Fibre Channel device port in a point-to-point or fabric connection.

Output Power LED

A power supply LED that indicates that the power supply is providing DC voltage to the switch. Applies only to SANbox2-16 and SANbox2-64 switches.

Over Temperature LED

A chassis LED or a power supply LED that indicates that the switch or power supply is overheating.

Pending Firmware

The firmware image that will be activated upon the next switch reset.

POST

Power On Self Test

Power On Self Test (POST)

Diagnostics that the switch chassis performs at start up.

Principal Switch

The switch in the fabric that manages domain ID assignments.

SANbox Manager

Switch management application.

SFP

Small Form-Factor Pluggable.

Small Form-Factor Pluggable

A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port.

SNMP

Simple Network Management Protocol

Soft Zone

Soft zoning divides the fabric for purposes of controlling discovery. Members of the same soft zone automatically discover and communicate freely with all other members of the same zone.

Target

A storage device that responds to an initiator device.

User Account

An object stored on a switch that consists of an account name, password, authority level, and expiration date.

VCCI

Voluntary Control Council for Interference

World Wide Name (WWN)

A unique 64-bit address assigned to a device by the device manufacturer.

WWN

World Wide Name

Zone

A set of ports or devices grouped together to control the exchange of information.

Zone Set

A set of zones grouped together. The active zone set defines the zoning for a fabric.

Zoning Database

The set of zone sets, zones, and aliases stored on a switch.

Index

A

access control list zone 3-15, 3-28
account name 3-3, A-1
active firmware 4-34
active zone set 3-12, 3-15, 4-25
Active Zoneset data window 3-12
Admin
  account name A-6
  authority A-6
admin authority 3-1
Admin command A-7
administrative state
  configured 4-22, 5-11
  current 4-22, 5-11
  port 5-11, A-46
  switch 4-22, A-31
alarm
  configuration 4-15, A-36
  configuration display A-65
  log A-30, A-53
alias
  add members 3-29, A-8
  copy A-8
  create 3-28, A-8
  delete A-8
  delete members A-9
  description 3-15
  display list A-8
  display members A-9
  remove 3-29
  rename A-9
Alias command A-8
Arbitrated Loop Physical Address A-46
archive configuration 4-30
authentication
  trap 4-28
  user A-50
authority A-6
auto save
  default fabric view file 2-14
  graphing options B-4
  zoning configuration 3-17

B

beacon A-30
BootP boot method 4-27
broadcast 4-24, A-53
browser
  location 2-14, B-4
  requirement 2-1

C

CD-ROM drive 2-1
chassis
  LEDs 4-36
  status A-53
Command Line Interface A-1
command syntax A-5
commands A-6
Config command A-10
configuration
  activate A-10
  archive 4-30
  backup A-10
  copy A-10
  delete A-10
  edit A-10
  list A-10
  reset A-25
  restore 4-30, A-11
  save A-11
configured administrative state 4-22
contact 4-28
CRC error 4-15
credits 5-14
current administrative state 4-22

D

data window
  Active Zoneset 3-12

Configured Zonesets 4-14
description 2-24, 2-27, 2-30
Name Server 4-8, 5-9
port information 5-7
port statistics 5-4
switch 4-10
database
fabric 3-3
zoning 3-19
date 4-17
Date command A-13
Decode error 4-15
default
configuration 4-32
user account 3-1
visibility 3-17, 3-23
zoning 3-18
default fabric view file
auto save 2-14
SANbox Manager 2-14
Detailed FDMI Display Dialog 4-10
device scan 5-14
disk space 2-1
distance 5-14
domain ID
description 4-23
display A-54
lock 4-23
donor port 5-2, 5-13, 5-14, A-54
Dynamic Host Configuration Protocol 4-27

E

E_Port
isolation 3-18, 4-23
self-discovery 5-13
Error Detect Timeout 4-26
Ethernet port 2-1
event browser
display 3-9
filter 3-11
preference 2-15
save to file 3-12
sort 3-12
event logging
by component A-43, A-68
by port A-44, A-69
by severity level A-68
display A-68
restore defaults A-44
save settings A-44
settings A-69
severity level A-44
start A-44
stop A-45
event severity 3-10
external test 5-16, A-76

F

F_Port 5-2, 5-12
fabric
add 3-3
add a switch 3-5
database 3-3
delete 3-4
discovery interval 2-14
displaying information 3-7
loop port 5-2, 5-12
management 3-1
merge 3-18
port 5-2, 5-12
rediscovery 3-5
security 3-1
status 3-7
tree 2-23
zoning 3-13
Fabric Device Management Interface A-54
fabric services 3-2
Fabric View
arrange graphs B-6
customize graphs B-6
display graphs B-5
preferences B-4
start B-2
fabric view file B-4
auto save B-4
open 3-4, B-3

password B-2
save 2-14, 3-4
faceplate display
data window 2-30
description 2-17, 2-28
open 2-26
popup menu 2-29
factory defaults 4-32, A-25
Fallback command A-14
Fan Fail LED 4-36
FC-4 descriptor 5-14
FC-SW-2 compliance 4-25
firmware
activate pending 4-35
active 4-34
change pending 4-35
fallback 4-35
image file 4-34, A-19
inactive 4-34
install with SANbox Manager 4-34
list image files A-19
non-disruptive activation 4-34, A-18
pending 4-34, A-14
remove image files A-19
retrieve image file A-19
unpack image A-19
version A-58
FL_Port 5-2, 5-12

G

gateway address 4-27
generic
loop port 5-13
port 5-2, 5-12
graphic window 2-24

H

hard reset 4-20
Hardreset command A-15
hardware status 4-36
Heartbeat LED 4-36
help 2-16
Help command A-16
History command A-17
host bus adapter A-54
hot reset 4-20
Hotreset command A-18

I

I/O Steam Guard 5-14
Image command A-19
inactive firmware 4-34
inband management 4-24
Initial Start Dialog 2-14
Input Power LED 4-36
internal test 5-16, A-76
IP
address 4-27
configuration 4-27
ISL monitoring 4-15

L

layout 2-26
legacy address format 4-25
link
delete 3-7
selecting 2-26
status 2-25
Link data window 4-13
link state database A-54
Lip command A-20
log
archive A-43
clear A-43
event A-43, A-68
power-on self test A-57
logged in users A-58
login
limit 3-4, A-2
monitoring 4-15
logout monitoring 4-15
loop port
bypass A-46
enable A-46
fabric 5-2, 5-12
generic 5-13

initialization A-20
loopback test 5-16
loss of signal monitoring 4-15

M

management workstation 2-1
manufacturer information A-73
media status 5-4
memory
activity A-54
workstation 2-1
menu structure 2-18
messages C-1

N

name server
display A-54
export 4-17
zone 3-14
Name Server data window 4-8, 5-9
network
configuration reset A-26
discovery 4-27
interfaces A-54
properties 4-26
node-to-node test 5-17
non-disruptive activation 4-35, A-18

O

online
help 2-16
test 5-17
online test A-76
operating systems 2-1
orphan zone set 3-15
Over Temperature LED 4-36

P

page break A-30
Passwd command A-21
password
change A-21
default fabric file B-4
default fabric view file 2-13
switch 3-3, A-21
user account 4-5, A-1
pending firmware 4-34, 4-35
performance graphs B-5
Ping command A-22
popup menu 2-26, 2-29
port
administrative state 5-11, A-46
buffer credits 5-13, 5-14
configuration 5-10, A-32
configuration display A-65
counters A-46
displaying information 5-1
donor 5-14
extending credits 5-14
external test A-76
initialize A-25
internal test A-76
loopback test A-76
mode 5-2
online test A-76
operational information A-55
operational state 5-3
performance A-55, A-71, B-1
recipient 5-14
reset 5-16
selecting 2-29
speed 5-3, A-46
status 2-28
test 5-16
view 2-15, 2-28
Port Information data window 4-13, 5-7
Port Statistics data window 4-13, 5-4
port/device tree 3-19
power on self test log A-57
preferences
Fabric View B-4
SANbox Manager 2-14
principal switch 4-23
processor 2-1
properties
network 4-26
port 5-10

Ps command A-23

Q

Quit command A-24

R

read community 4-28
receive buffer 5-13
recipient port 5-14
refresh 3-7, 4-8
Registered State Control Notification 5-14
remote logging 4-29
reset
  with POST 4-20
  without POST 4-20
Reset command A-25
Resource Allocation Timeout 4-26
restore configuration 4-30
Reverse Address Resolution Protocol 4-27

S

SANbox Manager
  default fabric file 2-6, 2-11
  exit 2-6, 2-11
  preferences 2-14, B-4
  uninstall 2-8, 2-13
  user interface 2-17
  version 2-16
SANbox Manager installation
  Linux 2-3, 2-9
  Solaris 2-4, 2-9
  Windows 2-2, 2-8
SANbox2-16 switch 3-8
SANbox2-8c switch 3-8
scan device 5-14
security 3-1
SerDes level test 5-16
serial port 2-1
Set command A-30
Set Config command A-32
Set Log command A-43
Set Port command A-46
Set Setup command A-48
severity levels 3-10
SFP level test 5-16
Show command A-53
Show Config command A-65
Show Log command A-68
Show Perf command A-71
Show Setup command A-73
Shutdown command A-75
Simple Network Management Protocol
  configuration 4-28, A-48
  configuration display A-73
  proxy 4-28
  reset A-25
  trap configuration 4-29
SNMP enabled 4-28
soft zone 3-14, 3-28
static boot method 4-27
status icon color 2-23
steering A-57
subnet mask address 4-27
switch
  add 3-5
  administrative state 4-22, A-31
  configuration 4-20, A-35
  configuration display A-65
  delete 3-7
  displaying information 4-7
  hard reset 4-20, A-15
  hot reset 4-20
  icons 3-7
  location 4-28
  manufacturer information A-73
  operational information A-58
  paging 4-17
  properties 4-21
  replace 3-6
  reset A-79
  reset without POST 4-20, A-25
  restore factory defaults 4-32
  selecting 2-26
  status 2-25
Switch data window 4-10
symbolic name 4-22
syslog 4-29

system configuration
  change A-49
  display A-73

T

temperature A-53
temperature threshold 4-18
Test command A-76
testing ports 5-16
time 4-17, A-13
timeout values 4-25
tool bar
  standard 2-22
  zoning 3-20
topology display
  arrange icons 2-26
  data windows 2-27
  description 2-17
  usage 2-25
transceiver status 5-4
trap
  authentication 4-28
  community 4-28
  configuration 4-29
  SNMP version 4-29

U

Uptime command A-79
user
  account A-1
  authentication A-50
  logged in A-58
user account
  create 4-3
  default 4-2
  modify 4-6
  password 4-5
  remove 4-4
  security 3-1
User command A-80

V

version 2-16

W

working
  directory 2-14, B-4
  status indicator 2-24
write community 4-28

Z

zone
  access control list 3-15
  add member port 3-26, A-84
  copy 3-23, A-84
  create 3-25, A-84
  definition 3-14
  delete A-84
  delete member port A-85
  list A-85
  list members A-85
  name server 3-14
  remove 3-23, 3-27
  remove all 3-27
  remove member port 3-27
  rename 3-27, A-85
  soft 3-14
  type 3-28, A-85
Zone command A-84
zone merge
  description 3-18
  failure 3-18
  failure recovery 3-18
zone set
  activate 3-23, A-88
  active 3-12, 3-15, A-90
  add member zone A-88
  copy A-88
  create 3-22, A-88
  deactivate 3-23, A-26, A-88
  definition 3-15
  delete A-88
  delete member zone 3-23, A-89
  display A-89
  display active A-88
  display members A-89
  display zones A-85

management 3-22
orphan 3-15
remove 3-24
rename 3-27, A-89
tree 3-19
Zoneset command A-88
zoning
configuration 3-17, A-37
configuration display A-65
database 3-16, 3-19, 4-25, A-26
default 3-18
edit A-90
history A-90
limits A-91
list definitions A-91
remove all 3-24
revert changes A-91
save edits A-91
Zoning command A-90

Notes